



# ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

## UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

CARRERA DE INGENIERÍA EN ELECTRÓNICA, REDES Y  
COMUNICACIÓN DE DATOS

“REINGENIERÍA DE LA RED DE DATOS DEL CENTRO DE  
ENTRENAMIENTO PARA EL ALTO RENDIMIENTO EN LA  
LOCALIDAD DE CARPUELA PROVINCIA DE IMBABURA”

JAVIER DAVID ESPINOSA HURTADO

Tesis presentada como requisito previo a la obtención del grado  
de: INGENIERO EN ELECTRÓNICA, REDES Y  
COMUNICACIÓN DE DATOS.

**SANGOLQUI, DICIEMBRE DEL 2014**

*Certificado de tutoría*

UNIVERSIDAD DE LAS FUERZAS ARMADAS  
ESPE  
INGENIERIA EN ELECTRONICA, REDES Y COMUNICACIÓN DE DATOS

**CERTIFICADO**

Ing. Carlos Romero Gallardo, Ing. Iván Patricio Vizcaíno E.

**CERTIFICAN**

Que el trabajo titulado denominado REINGENIERÍA DE LA RED DE DATOS DEL CENTRO DE ENTRENAMIENTO PARA EL ALTO RENDIMIENTO EN LA LOCALIDAD DE CARPUELA PROVINCIA DE IMBABURA realizado por Javier David Espinosa Hurtado, ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas de la Universidad de las Fuerzas Armadas-ESPE.

Debido a que el presente trabajo fue realizado bajo nuestra tutoría y seguimiento se recomienda su publicación.

El mencionado trabajo consta de [un] documento empastado y [dos] disco compacto el cual contiene los archivos en formato portátil de Acrobat (pdf). Autorizan a Javier David Espinosa Hurtado que lo entregue a Dr. Nikolai Espinosa, en su calidad de Director de la Carrera.

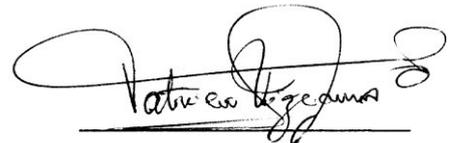
Sangolqui, 10 de diciembre de 2014.



Ing. Carlos Romero Gallardo

ID: L00007728

**DIRECTOR**



Ing. Ivan Patricio Vizcaino E.

ID: 100128290

**CODIRECTOR**

*Declaración de Responsabilidad*

UNIVERSIDAD DE LA FUERZAS ARMADAS-ESPE  
INGENIERIA EN ELECTRONICA, REDES Y COMUNICACIÓN DE DATOS  
DECLARACIÓN DE RESPONSABILIDAD

Javier David Espinosa Hurtado

DECLARO QUE:

El proyecto de grado denominado REINGENIERÍA DE LA RED DE DATOS DEL CENTRO DE ENTRENAMIENTO PARA EL ALTO RENDIMIENTO EN LA LOCALIDAD DE CARPUELA PROVINCIA DE IMBABURA, ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan el pie de las páginas correspondiente, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolqui, 10 de diciembre de 2014.



---

Javier David Espinosa Hurtado

*Autorización de publicación*

UNIVERSIDAD DE LAS FUERZAS ARMADAS  
ESPE  
INGENIERIA EN ELECTRONICA, REDES Y COMUNICACIÓN DE DATOS

### **AUTORIZACIÓN**

Yo, Javier David Espinosa Hurtado

Autorizo a la UNIVERSIDAD DE LA FUERZAS ARMANDAS-ESPE, la publicación, en la biblioteca virtual de la Institución del trabajo REINGENIERÍA DE LA RED DE DATOS DEL CENTRO DE ENTRENAMIENTO PARA EL ALTO RENDIMIENTO EN LA LOCALIDAD DE CARPUELA PROVINCIA DE IMBABURA, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolqui, 10 de diciembre de 2014.



---

Javier David Espinosa Hurtado

## DEDICATORIA

Quiero dedicar este proyecto de Tesis a Dios por guiar y forjar cada día mi camino, a mi familia Mi Esposa, mis hijas: Paulina, Cecilia y Victoria quienes han sido mi inspiración para culminar mi carrera, a mi Madre y mi Padre que han entregado su vida para educarme y formarme como un profesional exitoso. En el tiempo que me ha tomado la realización de esta tesis he presenciado la importancia del apoyo de la familia, en los momentos más difíciles, así como en los más felices llegan con su amor incondicional.

## AGRADECIMIENTO

Agradezco a Dios nuevamente, reconociendo que por sus enormes bendiciones he logrado todas las metas que me he propuesto. Agradezco a mis padres, a mi familia que con su amor y apoyo he llegado a culminar mi trabajo de tesis.

Quiero también agradecer al Arq. Italo Cordova Coordinador general de Infraestructura Deportiva del Ministerio del Deporte quien me autorizo para ingresar a las dependencias del complejo deportivo Carpuela para la realización del presente trabajo de tesis de grado.

Al Director de Carrera Dr. Nikolai Espinosa por su colaboración en el proceso de graduación, al Ing. Carlos Romero y al ing. Patricio Vizcaíno en calidad de Director y Codirector de la presente Tesis.

A cada profesor de la ESPE que tuve el agrado de conocer ya que cada experiencia en cada periodo académico he experimentado diversidades y triunfos que juntos, siento que me complementan como la profesional que soy hoy en día.

1	CAPÍTULO I: Introducción .....	1
1.1	Antecedentes. ....	1
1.2	OBJETIVOS.....	6
1.2.1	General.....	6
1.2.2	Específicos.....	6
1.3	JUSTIFICATIVO.....	8
1.4	ALCANCE DEL PROYECTO.....	9
2	CAPÍTULO 2. FUNDAMENTACIÓN TEÓRICA.....	12
2.1	INTRODUCCIÓN.....	12
2.2	ANTECEDENTES HISTÓRICOS DE LAS REDES [2].....	12
2.3	CONCEPTOS GENERALES DE REDES [3].....	13
2.3.1	Introducción.....	13
2.3.2	Concepto de Red.....	14
2.3.3	Ventajas de una Red de Computadoras.....	15
2.3.4	Conceptos y Funcionalidades Básicas.....	15
2.3.5	Tipos de Redes.....	19
2.3.6	Dispositivos de Interconexión.....	20
2.4	FUNDAMENTOS DE CONSTRUCCIÓN DE UNA RED LAN [4].....	22
2.4.1	INTRODUCCIÓN.....	22
2.4.2	ANTECEDENTES.....	22
2.4.3	CARACTERÍSTICAS DE UN SISTEMA DE CE [5].....	23
2.4.4	ORGANIZACIONES DE ESTANDARIZACIÓN.....	24
2.4.5	NORMAS Y ESTÁNDARES DE CE VIGENTES [13-16].....	25
2.4.6	COMPONENTES DE UN SISTEMA DE CE [60].....	32
2.4.7	TIPOS DE ETIQUETADO [52].....	36

3	CAPITULO 3. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED DE DATOS DEL COMPLEJO DEPORTIVO DE CARPUELA .....	38
3.1	INTRODUCCION .....	38
3.2	LEVANTAMIENTO DE INFORMACIÓN .....	39
3.2.1	DISTRIBUCION Y UBICACIÓN FISICA DE LOS PUNTOS .....	41
3.2.2	CABLEADO ESTRUCTURADO .....	44
3.2.3	ELEMENTOS DE PARTE ACTIVA .....	53
3.2.4	ESQUEMA DE LA TOPOLOGÍA DE RED ACTUAL .....	71
3.2.5	ESPECTRO WIFI .....	72
3.3	ANÁLISIS DE SITUACIÓN ACTUAL .....	73
3.3.1	CABLEADO ESTRUCTURADO .....	73
3.3.2	ELEMENTOS DE PARTE ACTIVA .....	82
3.3.3	ESQUEMA DE LA TOPOLOGÍA DE RED ACTUAL .....	84
3.3.4	ANÁLISIS ESPECTRAL WIFI .....	88
3.4	INCUMPLIMIENTO DE NORMAS Y ESTÁNDARES DE CABLEADO ESTRUCTURADO .....	88
3.4.1	CABLEADO HORIZONTAL .....	88
3.4.2	CABLEADO VERTICAL .....	90
3.4.3	CUARTOS DE TELECOMUNICACIONES .....	91
3.4.4	DATA CENTER .....	92
3.5	PARÁMETROS DE RENDIMIENTO DE LA RED ACTUAL .....	95
3.5.1	FLEXIBILIDAD .....	95
3.5.2	DISPONIBILIDAD .....	95
3.5.3	ESCALABILIDAD .....	96
3.5.4	RENDIMIENTO .....	96
3.5.5	DOMINIOS DE BROADCAST .....	97
3.5.6	SEGURIDAD .....	97
4	CAPITULO IV. DISEÑO DE TOPOLOGÍAS FÍSICA Y LÓGICA PARA LA RED DE DATOS .....	98

4.1	INTRODUCCIÓN .....	98
4.2	ESTUDIO DE LA PROYECCIÓN DE CRECIMIENTO DE RED EN LA INSTITUCIÓN [1] .....	98
4.3	POLÍTICAS EN LA RED .....	99
4.3.1	CUARTOS DE TELECOMUNICACIONES .....	99
4.3.2	DATACENTER .....	100
4.3.3	EQUIPAMIENTO ACTIVO Y SERVIDORES .....	100
4.3.4	RED INALÁMBRICA .....	101
4.3.5	EQUIPOS DE CÓMPUTO .....	101
4.4	ANÁLISIS DE REQUERIMIENTOS DE USUARIOS .....	101
4.5	REINGENIERÍA DE LA RED DE DATOS DEL CENTRO DE ENTRENAMIENTO PARA EL ALTO RENDIMIENTO DE CARPUELA. ....	103
4.5.1	CONSIDERACIONES DE DISEÑO .....	104
4.5.2	POLÍTICAS DE ADMINISTRACIÓN DE LA PARTE ACTIVA .....	110
4.5.3	MODELO DE RED .....	111
4.5.4	SEGMENTACIÓN Y DIRECCIONAMIENTO IP .....	128
4.5.5	MANEJO DE USUARIOS Y CONTRASEÑAS .....	138
5	CAPITULO V. SIMULACIÓN DEL DISEÑO DE TOPOLOGÍA LÓGICA DE LA RED DE DATOS DEL CENTRO DE ENTRENAMIENTO PARA EL ALTO RENDIMIENTO DE CARPUELA. ....	140
5.1	SIMULACIONES .....	140
5.1.1	TOPOLOGÍAS DE RED .....	142
5.1.2	CONFIGURACIONES BÁSICAS .....	144
5.1.3	CONFIGURACIÓN DE VLAN .....	153
5.1.4	CONFIGURACIÓN DE PUERTOS .....	155
5.1.5	CONFIGURACIÓN DEL PROTOCOLO OSPF .....	157
5.1.6	HABILITACIÓN DE ALTA DISPONIBILIDAD – PROTOCOLO SPANNING TREE .....	158
5.2	OBJETIVOS FUNCIONALES .....	160
5.2.1	SEGURIDAD .....	160

5.2.2	DISPONIBILIDAD .....	161
5.2.3	ESCALABILIDAD.....	162
5.2.4	DESEMPEÑO .....	162
5.2.5	FLEXIBILIDAD .....	163
6	CAPITULO VI. CONCLUSIONES Y RECOMENDACIONES .....	164
6.1	CONCLUSIONES .....	164
6.2	RECOMENDACIONES .....	168

## ÍNDICE DE FIGURAS

Figura 1 Vista General del Complejo.....	3
Figura 2 Esquema de red de Computadoras.....	14
Figura 3 El modelo OSI.....	16
Figura 4 Relación entre los dispositivos de red.....	21
Figura 5 Asignación de pines según norma.....	34
Figura 6 Características Fluke Network DTX-1800.....	48
Figura 7 Software LinkWare - Fluke Network.....	48
Figura 8 Router Cisco Serie 800.....	55
Figura 9 Switch 3Com serie 7700 .....	57
Figura 10 Switch 3Com serie 5500 .....	58
Figura 11 Switch HP 1910-24G.....	59
Figura 12 Switch HP 2910-24G .....	63
Figura 13 Access Point HP m200 .....	65
Figura 14 Topología de red Actual .....	71
Figura 15 FTT en tiempo real.....	72
Figura 16 Barrido del espectro de WIFI.....	73
Figura 17 Topología física de red interna.....	85
Figura 18 Modelo de red Propuesto.....	116
Figura 19 Nivel de Distribución.....	119
Figura 20 Nivel de Acceso.....	122
Figura 21 Segmentación de la Red en Vlan.....	132
Figura 22 Topología de red de Alta Disponibilidad.....	143
Figura 23 Topología de la red de Datos del complejo.....	144

## ÍNDICE DE TABLAS

Tabla 1. Distancias permitidas para el cableado vertical según el medio de transmisión utilizado .....	33
Tabla 2. Asignación del color según el tipo de terminación .....	36
Tabla 3. Lista de servidores con sus respectivas IP .....	52
Tabla 4. Lista de equipamiento activo con su respectiva IP .....	52
Tabla 5. Listado del equipamiento .....	54
Tabla 6. Equipos de control y seguridad.....	80
Tabla 7. Uso de CPU de los switches .....	83
Tabla 8. Lista de Vlan configuradas en el switch 3Com 7750 .....	84
Tabla 9. Vlan configuradas en los switches .....	86
Tabla 10. Resumen de requerimientos de red de la institución .....	102
Tabla 11. Nomenclatura utilizada para los bloques .....	105
Tabla 12. Nomenclatura utilizada para el tipo de servicio .....	106
Tabla 13. Nomenclatura utilizada para el número de PP .....	106
Tabla 14. Distribución de áreas para enrutamiento dinámico OSPF .....	113
Tabla 15. Direccionamiento IP para enlaces de la red de datos .....	114
Tabla 16. Direccionamiento IP para el nivel de acceso .....	131
Tabla 17. Asignación de ACL en función de la LAN.....	137
Tabla 18. Características equipamiento Cisco .....	142

## RESUMEN

El centro de entrenamiento para el alto rendimiento de Carpuela es uno de seis centros ubicados estratégicamente en la provincia de Imbabura y está orientado a recibir y alojar a atletas de alto nivel de todo el país. La red de datos de CEAR EP es la que se encarga de administrar todos los servicios informáticos de la empresa pública, por lo cual es importante que su infraestructura ofrezca alta disponibilidad y calidad de servicio, soportando grandes cantidades de tráfico, además de poseer escalabilidad, flexibilidad y seguridad. Este trabajo plantea una propuesta técnica que permite mejorar el desempeño de la red, proponiendo un esquema basado en un estudio pormenorizado de su infraestructura y requerimientos actuales, mediante la aplicación de un modelo jerárquico basado en el estudio por capas, y la microsegmentación a nivel lógico de la red, además de la implementación de un esquema que asegura la continuidad del servicio. La microsegmentación de red en cambio está basada en el estudio de la estructura orgánica, funciones, roles y recursos compartidos de los usuarios VLMS, considerando además un rango de crecimiento en función de la cantidad de usuarios presentes en cada una de las subredes.

### **Palabras clave:**

- Micro segmentación.
- Cableado Estructurado.
- Modelo Jerárquico.
- Núcleo Colapsado.
- Simulación.

## ABSTRACT

The training center for high performance Carpuela is one of six centers strategically located in the province of Imbabura and is oriented to receive and accommodate elite athletes from around the country. Among the services provided by the center are those used by the data network CEAR EP which is what is responsible for managing all IT services of the public company, so it is important that their infrastructure offers high availability and quality service, supporting large amounts of traffic, besides having scalability, flexibility and security. This paper presents a technical proposal that improves the network performance, proposing a system based on a detailed study of its infrastructure and current requirements by applying a hierarchical model based on the study layered schema and logic level microsegmentation network, in addition to implementing a scheme that ensures continuity of service. Microsegmentation network change is based on the study of organic structure, functions, roles and shared resources by users, using efficient addressing VLSMs, also considering a range of growth depending on the number of users present in each of subnets.

### **Keywords :**

- Micro segmentation.
- Structured Cabling.
- Hierarchical Model.
- Collapsed Core.
- Simulation.

## 1 **CAPÍTULO I: Introducción**

### **1.1 Antecedentes.**

El **"COMPLEJO DEPORTIVO PARA ENTRENAMIENTO DEL ALTO RENDIMIENTO EN LA LOCALIDAD DE CARPUELA"** se encuentra ubicado en la Panamericana Norte Km 45 vía a Tulcán, en el cantón Ibarra, Provincia de Imbabura.

En 8.1 hectáreas de extensión, Carpuela acogerá al deporte élite ecuatoriano, en el Centro de Entrenamiento para el Alto Rendimiento (CEAR) con instalaciones e implementos deportivos de primer nivel.

Además, la práctica deportiva se complementará con áreas administrativas, residencia, comedor, cocina, área de atención médica, área educativa y espacios de recreación, beneficiando a más 41.660 personas.

Su proceso constructivo se dividió en dos etapas: la primera desarrollada en los años 2007 al 2009 en donde se realizaron las estructuras básicas como conformación de plataformas y la construcción de los edificios: Administrativo, Coliseo de uso múltiple, residencia, canchas, camerinos, aulas, laboratorios y biblioteca.

La segunda etapa del proceso constructivo se ejecuta en el periodo de septiembre del 2011 a enero del 2013 etapa en la cual se ejecuta el

proyecto integral complementario el cual ya incluye un estudio de necesidades básicas en lo referente a conectividad de voz y datos. Se habla de necesidades básicas ya que al no existir un modelo de gestión lo que implemento fue solo una infraestructura básica consistente una red de conectividad en un medio de fibra óptica y el cableado horizontal hacia todas las dependencias de edificio administrativo, unidad educativa y bloque recreacional.

Se han analizado los aspectos arquitectónicos que tienen influencia directa en el diseño de las instalaciones de voz y datos, tales como acabados, tipo de uso de los diferentes ambientes, disposiciones generales sobre aspectos de seguridad y funcionalidad. (Ministerio Del Deporte Ecuador, 2014)

El “COMPLEJO DEPORTIVO PARA ENTRENAMIENTO DEL ALTO RENDIMIENTO EN LA LOCALIDAD DE CARPUELA” se encuentra formado por 20 módulos, Área verde y canchas deportivas de la siguiente manera:



**Figura 1: Vista General del complejo**

**Fuente:** (SECOB Servicio de Contratación de Obras, 2012)

- 1.- ADMINISTRACION: Planta Baja: Área de consultorios, fisioterapia, rehabilitación y Planta Alta: Administración General, Contabilidad, recursos humanos, Coordinación deportiva, archivo deportivo, Cuarto de Control.
- 2.- CANCELES Y VESTIDORES: Baños y área de vestidores.

- 3.- COLISEO DE USO MULTIPLE: Cancha deportiva con graderíos, camerinos, baños, en tres niveles de plantas, parqueadero.
- 4.- CANCHAS DE USO MULTIPLE.
- 5.- GRADERIOS EXTERIORES.
- 6.- GIMNASIO DE POTENCIACION: Cuadrilátero de box y 2 gimnasios oficina entrenadores.
  
- UNIDAD EDUCATIVA:
  - 7.- BLOQUE 1: Aulas, Laboratorio, Oficinas, en 2 plantas.
  - 8.- BLOQUE 2: Aulas y Oficinas en 2 plantas.
  - 9.- BLOQUE 3: Aulas , Biblioteca, Laboratorio, en 2 plantas.
- 10.- BATERIAS SANITARIA.
- 11.- CAMERINOS PISTA ATLETICA: camerinos y baños.
- 14.- COLISEO DE CONTACTO: 2 Rings, camerinos y baños.
- 15.- RESIDENCIA: Dormitorios en 2 plantas y piscina.
- 16.- SERVICIOS COMPLEMENTARIOS: Dormitorios, auditorio, área de lavado y planchado.
- 17.- RESTAURANTE: Comedor, Área de preparación de alimentos, bodegas y cuartos fríos.
- 18.- BLOQUE RECREACIONAL: Sala de juegos, cocina y comedor.
- 19.- CAMERINOS FUTBOL SINTETICO: camerinos y baños.
- 20.- CAMERINOS BEISBOL: camerinos y baños.
- AREAS VERDES: plazoletas, canchas abiertas, caminos periféricos.

El complejo desde su construcción cuenta con la infraestructura física instalada la cual hasta esta fecha no ha sido utilizada por falta de la definición de un modelo de gestión definitivo. Es por eso que a la fecha 1 de septiembre del 2014 por medio del decreto 439 se crea la Empresa Publica CEAR EP. Y se define su operación de la siguiente manera. El CEAR Carpuela forma parte de un conjunto de 6 complejos a nivel nacional los mismos que dependen de una sede ubicada en la ciudad de Guayaquil y se encuentra el núcleo de la red a nivel Nacional y desde donde se proveen los servicios de Internet y datos a travez de un enlace de fibra contratado con la Corporacion Nacional de Telecomunicaciones. CNT EP. El Presente trabajo contempla una propuesta de diseño de red para el Complejo Deportivo CEAR Carpuela Ubicado en la Ciudad de Ibarra Provincia de Imbabura.

## **1.2 OBJETIVOS**

### **1.2.1 General**

Realizar el diseño de la Red de Datos del “Complejo Deportivo Para Entrenamiento Del Alto Rendimiento En La Localidad De Carpuela”, mediante el uso eficiente de recursos existentes, infraestructura y diseños anteriores.

### **1.2.2 Específicos**

- Realizar el levantamiento de información de situación actual como el análisis de la misma, dentro de la cual se establecen las falencias y fortalezas de la red, sirviendo de base para el desarrollo del rediseño de red.
- Micro segmentar la red basándose en el estudio de la estructura orgánica, funciones, roles y recursos compartidos de los usuarios, utilizando un direccionamiento eficiente VLSM, considerando además un rango de crecimiento en función de la cantidad de usuarios presentes en cada una de las subredes.
- Brindar un nivel de seguridad adicional a la red, permitiendo limitar el tráfico en función de reglas para acceso establecidas.

- Asegurar la continuidad del servicio de red, la implementación de enlaces redundantes de conexión y la aplicación de un protocolo que asegure una topología libre de bucles, permite que la red se encuentre disponible a pesar de que alguno de sus enlaces físicos o equipos de conmutación fallen.
- Simular la funcionalidad del modelo previamente establecido mediante la utilización del software Packet Tracer 5.3.1 el cual brinda una interfaz que facilita validar las configuraciones realizadas, demostrando su operatividad en independencia de la tecnología de infraestructura utilizada.
- Brindar un nivel de seguridad a los datos según su jerarquía de importancia.

### 1.3 JUSTIFICATIVO

El **“COMPLEJO DEPORTIVO PARA ENTRENAMIENTO DEL ALTO RENDIMIENTO EN LA LOCALIDAD DE CARPUELA”** es un centro de entrenamiento de carácter público en el cual se ha planteado la meta de ser pionero en la región en lo referente a dar servicios especializados a Deportistas de alto nivel prestando servicios de:

Instalaciones especializadas de primera categoría.

Hospedaje.

Alimentación.

Servicio médico.

Área educativa.

Una vez concluida su obra física luego de un análisis de su estado se ha evidenciado que para darle la funcionalidad adecuada es necesaria una reingeniería de la red de datos para optimizar su funcionamiento.

Actualmente el complejo ha entrado en operación sin que se haya dado una solución completa en lo que respecta a la conectividad de voz y datos ya que se cuenta solo con interconexión sin ningún tipo de seguridades o determinación de servicios de red a prestar.

#### **1.4 ALCANCE DEL PROYECTO.**

El presente trabajo plantea un diseño que permite mejorar el desempeño de la red, proponiendo un esquema basado en un estudio pormenorizado de su infraestructura y requerimientos actuales, debido a que el Complejo Deportivo tiene únicamente una infraestructura física de la red funcionando a un nivel muy básico y se han generado necesidades nuevas para las cuales es necesario un replanteamiento general de todo el proyecto electrónico. Mediante la aplicación de un modelo jerárquico basado en el estudio por capas, y la micro segmentación a nivel lógico de la red, además de la implementación de un esquema que asegura la continuidad del servicio.

Para la aplicación del modelo jerárquico se realizará un estudio previo de las características del equipamiento existente bajo el cual posteriormente se estructura la nueva red y las configuraciones llevadas a cabo para el fin propuesto, teniendo también en cuenta criterios de apilamiento con lo que se eliminen las cascadas en la red, al manejarse varios switches como un switch más grande mejorando el rendimiento, flexibilidad y facilitando la administración de los mismos.

La micro segmentación de red en cambio está basada en el estudio de la estructura orgánica, funciones, roles y recursos

compartidos de los usuarios, utilizando un direccionamiento eficiente **VLSM**, considerando además un rango de crecimiento en función de la cantidad de usuarios presentes en cada una de las subredes.

Así también la aplicación de seguridad tanto mediante la aplicación de un protocolo seguro de conexión con el equipamiento activo, como el control del tráfico generado en las diferentes **VLAN** y el control a nivel de acceso a la red ligando tanto la dirección MAC e IP brindan un nivel de seguridad adicional a la red, permitiendo limitar el tráfico en función de reglas para acceso establecidas.

Con el fin de asegurar la continuidad del servicio de red, la implementación de enlaces redundantes de conexión y la aplicación de un protocolo que asegure una topología libre de bucles, permite que la red se encuentre disponible a pesar de que alguno de sus enlaces físicos o equipos de conmutación fallen.

Con el desarrollo de la simulación se demuestra la funcionalidad del modelo previamente establecido mediante la utilización del software Packet Tracer 5.3.1 el cual brinda una interfaz que facilita validar las configuraciones realizadas, demostrando su operatividad en independencia de la tecnología de infraestructura utilizada.

Así, la elaboración del presente proyecto brinda una solución eficiente para la Red de Datos del Complejo Deportivo bajo la cual se mejora las prestaciones y el servicio ofrecido hacia la red interna, considerando la infraestructura actual con la que cuenta la misma.

## **2 CAPÍTULO 2. FUNDAMENTACIÓN TEÓRICA**

### **2.1 INTRODUCCIÓN**

Este capítulo contiene la fundamentación teórica abarcada en el presente trabajo, el cual involucra los campos de las redes de comunicación y cableado estructurado. Su estudio previo brinda una idea general de los conceptos y parámetros que se manejan en el proyecto, permitiendo de esta manera comprender su contenido y dar una idea clara del mismo. Para el desarrollo de este capítulo primero se comenzará con una revisión del área de redes de comunicación para posteriormente continuar con el ámbito de los sistemas de cableado estructurado.

### **2.2 ANTECEDENTES HISTÓRICOS DE LAS REDES (CNNA, 2013)**

La historia de las redes comenzó en el año de 1957 cuando se creó en los Estados Unidos la Agencia de Investigación de Proyectos Avanzados **ARPA**, como un organismo afiliado al Departamento de Defensa con el fin de impulsar el desarrollo tecnológico; en sus inicios ARPA se dedicaba a la investigación de proyectos del tipo espacial y militar.

Posteriormente en el año de 1965 ARPA patrocinó un programa con el fin de analizar las redes de comunicación usando computadoras, este programa contaba con centros de investigación en varios lugares del país, los mismos que para comunicarse entre ellos contaban con un terminal que se conectaba directamente hacia las estaciones mediante una extensión,

naciendo allí la idea de que una computadora pudiese conectarse hacia cualquier lugar sin necesidad de contar con conexiones directas como hasta el momento; de esa forma surge **ARPANET**.

En 1969 se construyó la primera red ARPANET, constituida por cuatro nodos situados en la UCLA (Universidad de California en los Ángeles), SRI (Stanford Research Institute), UCBS (Universidad de California de Santa Bárbara, Los Ángeles) y la Universidad de UTAH, los mismos que constituyeron la primera red. Posterior a esto se abrieron varios centros de investigación en cooperación con el Departamento de Defensa para promover el desarrollo de la misma, sin embargo los científicos que trabajaron en el proyecto comenzaron a utilizarlo con fines de comunicación y charla personal incluida la ciencia ficción, con lo cual surge la necesidad de separar la investigación con fines militares y de comunicaciones, formándose las redes **MILNET** y ARPANET respectivamente. Adicional se crearon las redes **CSNET** y **BITNET**, pero todas ellas usaban como backbone principal ARPANET. ARPANET fue llamada luego ARPA-INTERNET y posteriormente INTERNET nombre con el cual se conoce en la actualidad a esta red de redes.

## **2.3 CONCEPTOS GENERALES DE REDES (García, 1994)**

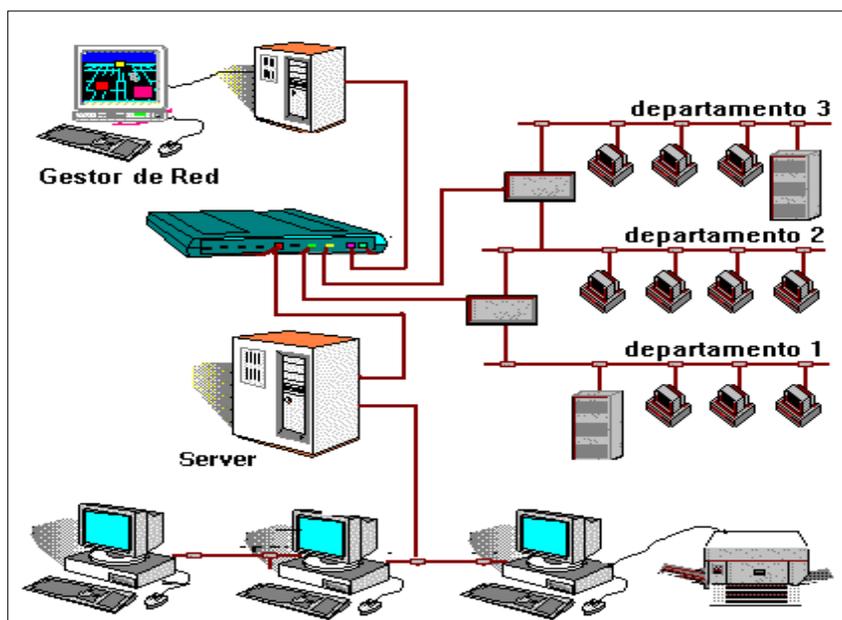
### **2.3.1 Introducción**

La difusión de las computadoras ha impuesto la necesidad de compartir información, programas, recursos, acceder a otros sistemas informáticos

dentro de la empresa y conectarse con bases de datos situadas físicamente en otras computadoras. En la actualidad, una adecuada interconexión entre los usuarios y procesos de una empresa u organización, puede constituir una clara ventaja competitiva. La reducción de costes de periféricos, o la facilidad para compartir y transmitir información son los puntos claves en que se apoya la creciente utilización de redes.

### 2.3.2 Concepto de Red

Una red es un conjunto de computadoras conectados entre sí, que pueden comunicarse compartiendo datos y recursos sin importar la localización física de los distintos dispositivos (ver **Fig. 2**).



**Fig. 2** Esquema de una Red de Computadoras

Fuente: (Garcia, 1994)

Cada dispositivo activo conectado a la red se denomina nodo. Un dispositivo activo es aquel que interviene en la comunicación de forma autónoma, sin estar controlado por otro dispositivo.

### **2.3.3 Ventajas de una Red de Computadoras**

Dependiendo de la topología de red que se estudie, se tienen las siguientes ventajas:

- Necesidad de compartición de recursos (equipamientos e información).
- Proceso Distribuido.
- Sistemas de Mensajería.
- Bases de Datos.
- Creación de grupos de trabajo.
- Gestión centralizada.
- Seguridad.
- Acceso a otros sistemas operativos.
- Mejoras en la organización de la empresa.

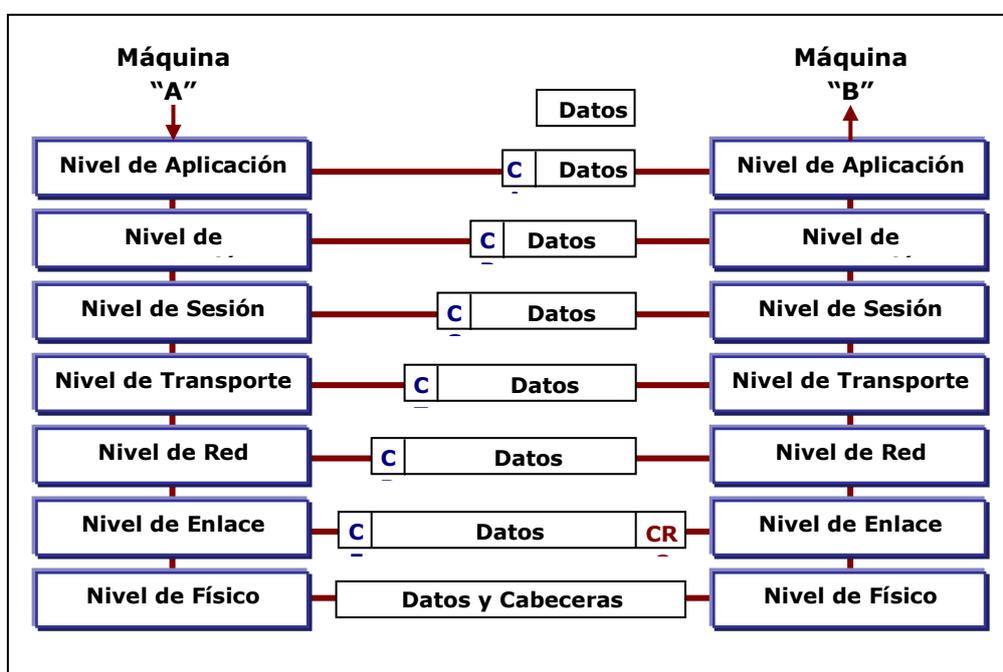
### **2.3.4 Conceptos y Funcionalidades Básicas**

#### **2.3.4.1 Modelo de referencia OSI (Gerónimo, 2007)**

Con objeto de proporcionar un estándar de comunicación entre diversos fabricantes, la Organización Internacional de Estándares (**ISO**, *International Standards Organization*) ha establecido una

arquitectura como modelo de referencia para el diseño de protocolos de Interconexión de Sistemas Abiertos (**OSI**, *Open Systems Interconnection*).

Este **modelo de siete niveles** proporciona un estándar de referencia para la intercomunicación entre sistemas de computadoras a través de una red utilizando protocolos comunes.



**Fig. 3 Modelo OSI**

**Fuente:** (García, 1994)

- 1) **Nivel Físico:** especifica un conjunto de estándares que definen aspectos mecánicos, eléctricos y funcionales para la conexión de los equipos al medio físico empleado. Su función es la transmisión de una cadena continua de bits a través de un canal básico de comunicación.

- 2) **Nivel de Enlace**: a partir del servicio de transmisión de bits ofrecido por el Nivel Físico, la tarea del Nivel de Enlace es ofrecer un control de errores al Nivel de Red. Además de la detección y corrección de errores, este nivel fragmenta y ordena en paquetes los datos enviados, también realiza funciones básicas de control de flujo.
  
- 3) **Nivel de Red**: este nivel proporciona los medios adecuados para establecer, mantener y terminar conexiones entre sistemas. El Nivel de Red principalmente permite direccionar los paquetes de datos que recibe del nivel de transporte.
  
- 4) **Nivel de Transporte**: se encarga de facilitar una transferencia de datos fiable entre nodos finales, proporcionando una integridad de los datos y una calidad de servicio previamente establecida.
  
- 5) **Nivel de Sesión**: Permite establecer, gestionar y terminar sesiones entre aplicaciones. Realiza la gestión y recuperación de errores y en algunos casos proporciona múltiples transmisiones sobre el mismo canal de transporte.

6) **Nivel de Presentación**: proporciona a las aplicaciones transparencia respecto del formato de presentación, realizando conversión de caracteres, códigos y algunas funciones de seguridad (encriptación).

7) **Nivel de Aplicación**: se denomina también “*nivel de usuario*” porque proporciona la interfaz de acceso para la utilización de los servicios de alto nivel.

#### 2.3.4.2 Topologías (ELIE, 2010)

La topología de una red es la configuración formada por sus *nodos* (estaciones) y las *interconexiones* existentes entre ellos (bus, estrella, anillo, etc.).

#### 2.3.4.3 Protocolos de comunicaciones

Los protocolos de comunicaciones son reglas y procedimientos utilizados en una red para establecer la comunicación entre los nodos. En los protocolos se definen distintos niveles de comunicación. Las reglas de nivel más alto definen ¿cómo se comunican las aplicaciones?, mientras que las de nivel más bajo definen ¿cómo se transmiten? las señales por el cable.

Los protocolos de comunicaciones se pueden clasificar en cuatro tipos:

- PROPIETARIOS
- XNS

- OSI
- TCP/IP

### **2.3.5 Tipos de Redes**

Dependiendo del territorio que una red abarca se clasifica en:

#### **2.3.5.1 Red de Area Local (LAN, *Local Area Network*)**

Una Red de Area Local está normalmente restringida a un área geográfica de tamaño limitado, como un edificio de oficinas y depende de un canal físico de comunicaciones con una velocidad media/alta y con una tasa de errores reducida.

#### **2.3.5.2 Red de Area Extensa (WAN, *Wide Area Network*)**

Una Red de Area Extensa es una red que ofrece servicios de transporte de información entre zonas geográficamente distantes. Es el método más efectivo de transmisión de información entre edificios o departamentos distantes entre sí.

#### **2.3.5.3 Red de Area Metropolitana (MAN, *Metropolitan Area Network*)**

Una red de área metropolitana es una red de alta velocidad (banda ancha) que dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado de cobre a velocidades que van desde los 2 Mbps hasta 155 Mbps (Megabits por segundo).

El concepto de red de área metropolitana representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas de una cobertura superior que en algunos casos no se limitan a un entorno metropolitano sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana.

### **2.3.6 Dispositivos de Interconexión (Jimenez, 2012)**

#### **2.3.6.1 Funciones básicas**

Para superar las limitaciones físicas de los elementos básicos de una red, existen dispositivos cuyas funciones son las de extender las topologías de red. Estos elementos son: *concentradores o hubs, repetidores, bridges o puentes, routers o encaminadores y gateways o pasarelas*.

Los dispositivos de interconexión de redes proporcionan algunas (o todas) de las siguientes funciones básicas:

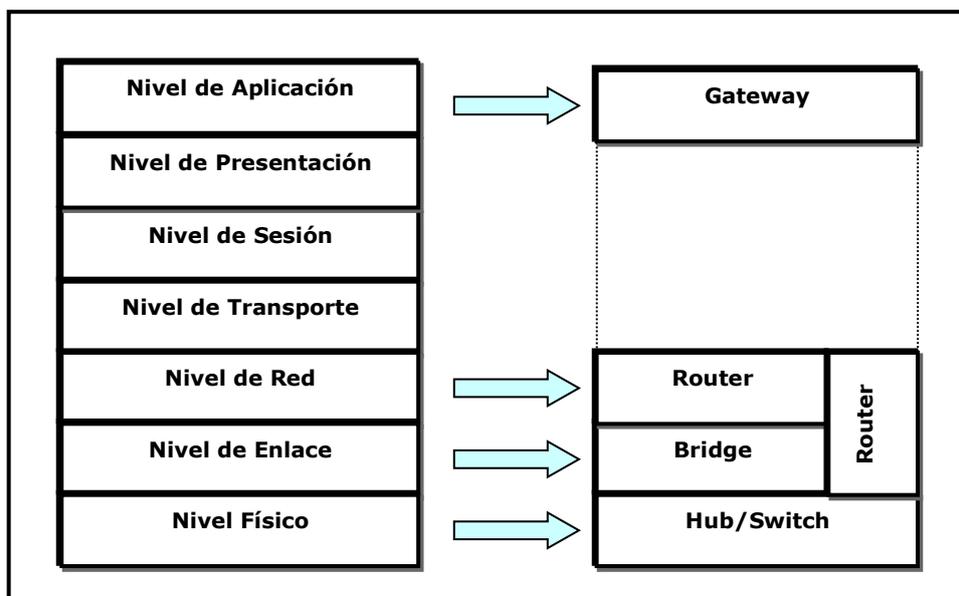
- a) Extensión de la red:** Permite ampliar el rango de distancia que puede alcanzar una red.
  
- b) Definición de segmentos dentro de la red:** Al dividir la red en segmentos se consigue aumentar las prestaciones de la red ya que cada tramo soporta sólo su propio tráfico y no los de los otros segmentos.

c) **Separación entre redes:** Mediante estos dispositivos las grandes redes se pueden componer de otras más pequeñas interconectadas entre sí, de forma transparente para el usuario. Varias redes físicas pueden combinarse para formar una única red lógica.

### 2.3.6.2 Características Principales

Los dispositivos de interconexión deben funcionar para cualquier tipo de red y tener una arquitectura estándar para los protocolos de comunicación de las redes.

La **figura 2.3** muestra la relación de los dispositivos de interconexión con los niveles del modelo de referencia OSI.



**Fig 4 Relación entre los dispositivos de interconexión y los niveles del modelo OSI**

**Fuente:** (Carrero, 2011)

## **2.4 FUNDAMENTOS DE CONSTRUCCIÓN DE UNA RED LAN (TIA/EIA, 2002)**

### **2.4.1 INTRODUCCIÓN**

Un sistema de cableado estructurado es una de las partes fundamentales de cualquier edificación, ya que soporta aplicaciones como voz, video y datos, constituyéndose en la base para la operación de todos los sistemas, al ser una de las partes vitales de la red. Es importante tener en cuenta que los sistemas de cableado estructurado tienen una duración aproximada de 15 años por lo que su diseño debe permitir y facilitar futuros cambios o ampliaciones en la red, teniendo en cuenta una debida planificación de crecimiento sobre la red actual.

### **2.4.2 ANTECEDENTES**

En sus inicios los edificios eran construidos tomando en cuenta dos servicios básicos, telefonía y red de datos. Sin embargo al no contar con estándares para su uso e instalación, los proveedores de equipamiento realizaban instalaciones de cable de acuerdo a sus necesidades, lo cual dificultaba en gran manera el cambio de proveedor para los clientes, ya que si se utilizaba nuevo equipamiento éste necesitaba de otras conexiones de red, obligándole al cliente a continuar con el antiguo proveedor o gastar grandes cantidades de dinero para realizar una nueva instalación de cable. Además las conexiones de red realizadas no brindaron flexibilidad ya que no se adaptaban a los cambios en una organización, así también si se necesita

añadir un servicio a la red era necesario añadir una nueva conexión de red, y hacer esto cada vez que se necesite añadir servicios a la misma.

En base a estas complicaciones que se presentaron tanto para proveedores como clientes, se hace necesario la creación de estándares que garanticen el funcionamiento de la red independientemente del proveedor, brindando compatibilidad entre los productos y que además se ajuste a los requerimientos de red y soporten las aplicaciones actuales y futuras en una red teniendo en cuenta un período de al menos 10 años.

#### **2.4.3 CARACTERÍSTICAS DE UN SISTEMA DE CE (Armendáriz, 2009)**

Un sistema de cableado estructurado se caracteriza por: Administración centralizada.- permite realizar una fácil localización de daños o averías y una rápida corrección de daños sin que la red quede completamente fuera de servicio. Flexibilidad.- debido al cambio constante de los ambientes de trabajo un sistema de **CE** permite configurar nuevos puestos de trabajo, modificando solo el enlace deseado. Reducción de costos de instalación y mantenimiento.- debido a que su administración e instalación se realiza en un entorno centralizado se reducen los costos en la instalación, así también su mantenimiento se simplifica. Solución segura: al contar con cuartos de telecomunicaciones se protege el corazón de la red, al resguardarlo de accesos no autorizados, pero además se brinda el acceso y facilidad de conexión de las estaciones de trabajo hacia las tomas de comunicaciones. Todo sistema de cableado estructurado se basa en normas y estándares que facilitan la administración detección y resolución de problemas de

comunicaciones debido a que estas normas brindan los lineamientos para su instalación y administración.

#### 2.4.4 ORGANIZACIONES DE ESTANDARIZACIÓN



**ISO.-** La Organización Internacional de Estándares (*International Standards Organization*) es una organización no gubernamental cuya función se centra en el desarrollo y publicación de estándares de calidad con la finalidad de facilitar el comercio a nivel mundial en lo relacionado a bienes y servicios, desarrollo científico, intelectual, tecnológico y económico.

Para la aceptación de un estándar se realiza un proceso que garantiza su aceptación.



**IEEE.-** El instituto de Ingenieros Eléctricos y Electrónicos (*The Institute of Electrical and Electronics Engineers*) es una sociedad que desarrolla estándares para las industrias eléctricas y electrónicas, particularmente en el área de redes de datos. El IEEE promueve la creatividad, el desarrollo y la integración, además de compartir y aplicar los avances en las tecnologías de la información, electrónica y ciencias en general.



**ANSI:** El Instituto Nacional Americano de Normalización (American National Standards Institute) es una organización privada sin fines lucrativos que administra y coordina la normalización voluntaria y las actividades relacionadas a la evaluación de conformidad en los Estados Unidos. Su principal objetivo es mejorar tanto la competitividad mundial de las empresas estadounidenses, así como la calidad de vida de los mismos, promoviendo y facilitando normas voluntarias de consenso y sistemas de evaluación de conformidad y protegiendo su integridad.



**EIA:** La Alianza de Industrias Electrónicas (Electronic Industries Alliance) es una organización comercial acreditada por la ANSI que desarrolla normas y publicaciones sobre las principales áreas técnicas: los componentes electrónicos, información electrónica, telecomunicaciones y seguridad de internet.

#### **2.4.5 NORMAS Y ESTÁNDARES DE CE VIGENTES (Carrero, 2011)**

Todo sistema de cableado estructurado se rige en base a lineamientos para su buen funcionamiento, dentro de las normas de cableado estructurado están: **ANSI/TIA/EIA-568-B: Estándar de cableado de telecomunicaciones para edificios comerciales.**

- ***TIA/EIA-568-B.1: Requerimientos generales.***

Especifica criterios básicos para que un sistema de cableado estructurado brinde funcionalidad ante multi-productos y multi-vendedor, mediante la planificación e instalación de un sistema estructural de cableado.

Este estándar además establece los criterios técnicos de configuración de un sistema de cableado estructurado, el acceso y conectorización de los elementos, estudiando cada uno de los componentes de un SCE49, requerimientos de instalación y los test necesarios para su buen funcionamiento.

- ***TIA/EIA-568-B.2: Componentes de cableado par trenzado balanceado.***

El rendimiento de una transmisión depende principalmente de las características del cableado horizontal, conectores utilizados, patch cords empleados, los cuidados que se tengan durante su instalación y el mantenimiento que se brinde al mismo, este estándar trata sobre los elementos que intervienen en la instalación del cableado par trenzado para que cumpla con los parámetros mínimos para una transmisión y buen rendimiento teniendo en cuenta los criterios que se establecen para su funcionamiento.

- ***TIA/EIA-568-B.3: Estándar de componentes de cableado de fibra óptica.***

El estándar especifica los componentes y requerimientos de transmisión en un sistema de cableado de fibra óptica tanto

multimodo como monomodo y los cables reconocidos, estudiando la conectorización del hardware, patch cords, e instrumentos de verificación.

- **ANSI/TIA/EIA-569: Estándar de recorridos y espacios en edificios comerciales de telecomunicaciones.** En este estándar se reconocen tres conceptos básicos: Los edificios son dinámicos, en el transcurso de su vida útil se producen continuas remodelaciones del espacio, constituyéndose esto en una regla. Tanto los medios de transmisión como los equipos de telecomunicaciones cambian dramáticamente, independientemente de su fabricante. Las telecomunicaciones implican más que voz y datos, se incluyen además sistemas de control, seguridad, audio, televisión, sensores, alarmas e intercomunicadores, inclusive servicios inalámbricos y también la transmisión de datos por medio de cables del sistema eléctrico. Es muy importante considerar que para que un edificio se adapte al sistema de telecomunicaciones su diseño debe incorporarse en la etapa de diseño arquitectónico, incluyéndose los diseños de rutas y espacios de telecomunicaciones que puedan adaptarse a las futuras necesidades de sus ocupantes.
- **ANSI/TIA/EIA-606-A: Estándar de administración de infraestructuras de telecomunicaciones comerciales.** El estándar provee una guía para la administración y el mantenimiento de la infraestructura de telecomunicaciones. Su administración se la divide

por clases; la clase 1 es para edificios simples, los cuales brindan servicio desde un único cuarto de equipos; la clase 2 se la utiliza para edificios sencillos que tienen un cuarto de equipos y varios cuartos de telecomunicaciones; la clase 3 es utilizada para campus con varios edificios interconectados y la clase 4 es para ambientes multicampus. Además el estándar establece la identificación de cada uno de los componentes y subsistemas basados en colores, códigos y etiquetas los cuales permitan identificar fácilmente cada uno de los servicios implementados.

- **ANSI/TIA/EIA-J-STD-607-A: Requerimientos de puesta a tierra para la infraestructura de telecomunicaciones en edificios comerciales.** Esta norma especifica como debe realizarse la conexión del sistema de tierras, frecuentemente un sistema de puesta a tierra es diseñado e instalado luego que el edificio ha sido construido y equipado. Su diseño debe soportar una infraestructura independiente del vendedor y de los productos empleados. Además es importante considerar que las infraestructuras actuales deben soportar las múltiples aplicaciones de un sistema de cableado estructurado.
- **ANSI/TIA/EIA-TSB-67: Especificación para la prueba en el campo del rendimiento de transmisión de sistemas de cableado de par trenzado sin blindaje.** Mediante el boletín técnico se detalla las

especificaciones y procedimientos para la validación y certificación del cableado estructurado ya instalado en una edificación. El boletín establece como marco de referencia dos tipos de configuraciones de verificación por enlace básico o canal; estos dos tipos de configuraciones se diferencian básicamente por los componentes que incluyen su configuración, en el caso del canal se abarca tanto el enlace permanente como los patch cord de conexión utilizados en el ambiente de trabajo, en cambio en el caso del enlace no se consideran los patch cord sino más bien enlaces de prueba. Los parámetros que se analizan en la certificación del cableado estructurado son los siguientes:

**Mapa de Cableado:** realiza una verificación de las terminaciones pin a pin, además de verificar errores de conectividad en las instalaciones.

- Por cada uno de los conductores el mapa de cableado indica.
- Continuidad con el extremo remoto.
- Pares reversos
- Pares divididos
- Pares transpuestos
- Cualquier otro defecto de conexión.
- Su correcta conectividad está basada en la norma ANSI/TIA/EIA-568-

B.2

**Longitud:** la longitud física del enlace está definida por la suma de los enlaces independientes existentes entre dos puntos finales. La longitud máxima de un enlace permanente es de 90m.

**Pérdida de inserción:** es medida por la pérdida de señal en un enlace permanente. Ésta se origina por la pérdida de energía eléctrica en la resistencia del cable.

Su valor se mide en dB, para valores más bajos de atenuación se tiene un mejor rendimiento del cable.

**Pérdida de Retorno:** se mide como la diferencia entre la potencia de la señal transmitida y la potencia de las reflexiones de la señal causadas debido a las variaciones en la impedancia de la señal. Los valores altos indican que los cables son más eficientes para la transmisión de señales en una red LAN ya que se pierde poca señal por causa de reflexiones.

**Pérdida de paradiafonía NEXT50:** o interferencia de extremo cercano. Causada por la interferencia de señales cercanas de un par de cables en otro par cercano.

El NEXT se expresa en dB, para valores más altos de NEXT se tiene menor interferencia en la señal y un mejor rendimiento del cable utilizado.

**Pérdida de paradiafonía por suma de potencia (PSNEXT51):** es la combinación de forma estadística del crosstalk recibido de los pares desde los extremos cercanos que operan simultáneamente.

**Pérdida de paradiafonía en el extremo lejano por igualación de nivel (ELFEXT52):** indica la relación entre el FEXT53 y la atenuación. Es una medida expresada en dB, influida por el trenzado de los cables, el Apantallamiento, así también la frecuencia de trabajo y la longitud del enlace. Un nivel alto de ELFEXT indica una buena transmisión del enlace.

**Pérdida de paradiafonía en el extremo lejano por igualación de nivel y suma de potencia (PSELFEXT54):** es una medida que se deriva del cálculo de las medianas del ELFEXT de cada par de cables. Su medida se encuentra influenciada por el trenzado de los cables, su apantallamiento, además de la frecuencia de trabajo y la longitud del enlace. Un valor alto de esta medida está relacionado a una buena transmisión en el enlace.

**Retardo en la propagación:** indica el tiempo en que una señal tarda en propagarse de un extremo a otro.

**ACR:** indica la relación entre la atenuación y la interferencia. Un valor alto de ACR indica que las señales recibidas son mucho más grandes que la interferencia, o que se tiene un NEXT alto y valores de atenuación bajos.

## 2.4.6 COMPONENTES DE UN SISTEMA DE CE (Manyari, 2008)

Un sistema de cableado estructurado está compuesto por varios componentes como se explica a continuación, en base a la norma ANSI/TIA/EIA-568-B.

### 2.4.6.1 Subsistema horizontal

El cableado horizontal es aquel que se extiende desde el cuarto de telecomunicaciones hasta la toma ubicada en el área de trabajo. Este subsistema incluye el cable horizontal, conectores, terminaciones, patch cords, puntos de consolidación y la ductería. Dentro de los servicios y sistemas más comunes considerados dentro del cableado horizontal están: servicios de voz de telecomunicaciones, equipamiento local de conmutación, comunicaciones de datos, redes LAN, servicios de video y otros relacionados a sistemas de señalización en construcciones.

La distancia máxima permitida en un sistema de cableado horizontal es de 90m, dentro de los cables reconocidos en la norma están el cable UTP de 100 ohmios categoría 3 o superior (categoría 5e o 6 recomendada) y/o cables de dos o más fibras ópticas multimodo.

### 2.4.6.2 Subsistema Vertical

Su función es proporcionar la interconexión entre cuartos de telecomunicaciones, cuartos de equipos y facilitar la entrada del cableado de telecomunicaciones. Este cableado incluye cables de **backbone**, conexiones cruzadas principales e intermedias, mecanismos de terminación, **patch cord**

o **jumpers** usados para la conexión de **backbone** a **backbone**, incluyendo además la interconexión entre edificios. El sistema de cableado vertical o de **backbone** usa una topología jerárquica en estrella ya que esta permite flexibilidad y fáciles variaciones, debiendo tenerse no más de dos niveles, porque de esta manera se limita la degradación de la señal en sistemas pasivos y además simplifica los movimientos, adiciones o cambios. Los medios de transmisión permitidos en este tipo de cableado son: Cable par trenzado **multipar** de 100 ohmios, cable de fibra óptica **multimodo** entre 62,5/125um, 50/125um o cable de fibra óptica **monomodo**; las distancias de cableado vertical permitidas se pueden observar en la siguiente tabla:

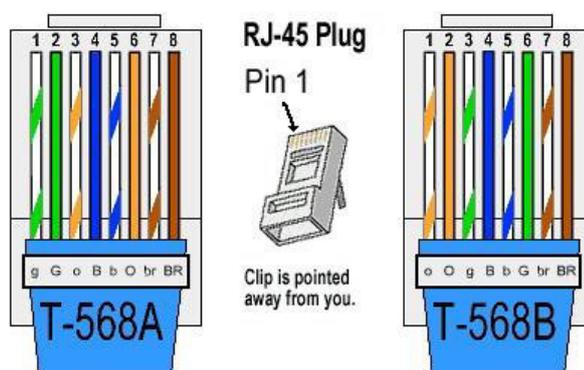
**Tabla 1. Distancias permitidas para el cableado vertical según el medio de transmisión utilizado**

Tipo de Medio	Alcance
Par trenzado 100 ohmios (transmisiones de voz)	Máximo 800m
Cable multipar cat. 3 de 100 ohmios	90m a 16MHz
Cable multipar cat. 5e de 100 ohmios	90m a 100MHz
Fibra óptica de 62,5/125 um	Máximo 2000m
Fibra óptica de 50/125 um	Máximo 2000m
Fibra óptica monomodo	Máximo 3000m

Fuente: (Manyari, 2008)

### 2.4.6.3 Área de trabajo

El área de trabajo se ubica desde la toma de telecomunicaciones hasta el equipo del usuario. El cableado en el área de trabajo debe estar diseñado para permitir una fácil adición, modificación o cambio ya que estas tomas no necesariamente son permanentes. Para la salida del conector de cable UTP o ScTP de cuatro pares se utilizan jack modulares de ocho posiciones, cuya asignación de pines puede definirse en base a las normas:



**Figura 5. Asignación de pines según la norma aplicada**  
**Fuente:** (CCNA, 2011)

Los cables de conexión utilizados en el área de trabajo no deben exceder los 5 metros y dependiendo de la aplicación puede ser necesario utilizar ciertos componentes como: cable especial o adaptador, adaptador en Y, adaptadores pasivos, adaptadores activos, entre otros.

Además es importante considerar que dentro de las áreas de trabajo también se debe considerar el caso del cableado en las denominadas oficinas abiertas, las cuales manejan una infraestructura modular muy susceptible a cambios, en las cuales cuando se realizan cambios se debe desechar todo el cableado retirado; sin embargo para evitar estos acontecimientos se implementan los MUTOAs (Multi-User Telecommunications Outlet Assembly) con lo cual se tiene la terminación de todos los cables horizontales en un lugar fácilmente accesible por todas las estaciones de trabajo, dando servicio a un máximo de 12 estaciones de trabajo. Los MUTOAs no deben estar instalados en pisos o techo falso ya que su ubicación será permanente.

#### **2.4.6.4 Cuarto de Telecomunicaciones**

Los cuartos de telecomunicaciones comprenden un área específica para los equipos de telecomunicaciones e incluyen las terminaciones del cableado vertical y horizontal, sistemas de seguridad, audio, televisión por cable, entre otros sistemas de telecomunicaciones. Los cuartos de telecomunicaciones no pueden contener instalaciones eléctricas que no sean propios de los sistemas de telecomunicaciones, además es necesario que los mismos cuenten con reguladores y **UPS** ante fallas de energía. Así también en los cuartos de telecomunicaciones debe proveerse un ambiente controlado, verificando su temperatura y humedad.

#### **2.4.6.5 Cuarto de Equipos**

Un cuarto de equipos se diferencia de un cuarto de telecomunicaciones por la naturaleza y complejidad del equipamiento. Un cuarto de equipos puede brindar alguno o todos los servicios de un cuarto de telecomunicaciones. En un cuarto de equipos además se cuenta con un espacio adicional para estaciones de trabajo del personal de Administradores. Toda edificación debe contar con al menos un cuarto de equipos o cuarto de telecomunicaciones dependiendo de la densidad de usuarios.

#### **2.4.6.6 Cuarto de Entrada de Servicios**

El cuarto de entrada de servicios abarca a todos los servicios de entrada de telecomunicaciones al edificio, incluyendo conectividad de hardware,

dispositivos de protección y el equipamiento necesario para facilitar la entrada del cableado.

#### 1.8.6.7 Sistema de Puesta a tierra

Todo sistema de cableado estructurado debe tener un sistema de puesta a tierra basado en el estándar ANSI/EIA/TIA-607.

**2.4.7 TIPOS DE ETIQUETADO** En base a la norma EIA/TIA-606 de acuerdo a la etiquetación se especifica que tanto el tamaño, como el color y el contraste deben ser seleccionados cuidadosamente de modo que la identificación sea fácilmente leída. El etiquetado realizado debe ser visible durante la instalación y el mantenimiento. Además para facilitar su identificación se ha especificado un color según el tipo de terminación como se puede observar en la siguiente tabla:

**Tabla 2. Asignación del color según el tipo de terminación**

<b>Tipo de Terminación</b>	<b>Color</b>
Punto de demarcación	Naranja
Conexión de red	Verde
Equipamiento	Purpura
Sistema Clave	Rojo
Primer nivel de Backbone	Blanco
Segundo nivel de Backbone	Gris
Backbone entre edificios	Café
Horizontal	Azul
Otros (alarmas sistemas de seguridad,..)	Amarillo

**Fuente:** (McGraw-Hill, 2008)

Su etiqueta debe permitir una fácil identificación de los componentes del sistema de cableado estructurado así como su ubicación por lo cual es muy importante que el diseño de su inscripción sea tratado cuidadosamente.

### **3 CAPITULO 3. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED DE DATOS DEL COMPLEJO DEPORTIVO DE CARPUELA**

#### **3.1 INTRODUCCION (Ministerio Del Deporte Ecuador, 2014)**

El **"COMPLEJO DEPORTIVO PARA ENTRENAMIENTO DEL ALTO RENDIMIENTO EN LA LOCALIDAD DE CARPUELA"** se encuentra ubicado en la Panamericana Norte Km 45 vía a Tulcán, en el cantón Ibarra, Provincia de Imbabura.

En 8.1 hectáreas de extensión, Carpuela acogerá al deporte élite ecuatoriano, en el Centro de Entrenamiento para el Alto Rendimiento (CEAR) con instalaciones e implementos deportivos de primer nivel.

En este sentido y en función de contar con Centros de Entrenamiento del más alto nivel, se establece la necesidad de estructurar un modelo de gestión que asegure el éxito y su óptima operación. Para ello se realizó un análisis complementario del estudio de consultoría "PROYECTO MODELOS DE GESTIÓN PARA LA OPERACIÓN DE LOS CENTROS DE ENTRENAMIENTO", reformulándose el propósito y grupos objetivos, con lo cual se establece el presente Modelo de Gestión para los Centros de Entrenamiento para al Alto Rendimiento de Carpuela (Imbabura), Cuenca (Azuay), Duran (Guayas), Macas (Morona Santiago) y Rioverde (Esmeraldas).

El modelo servirá además como documento marco, el cual se podrá aplicar a otros centros construidos con iguales o similares características en el país.

Se han analizado los aspectos arquitectónicos que tienen influencia directa en el diseño de las instalaciones de voz y datos, tales como acabados, tipo de uso de los diferentes ambientes, disposiciones generales sobre aspectos de seguridad y funcionalidad.

Debido a las características de los servicios, es necesario que la red cuente con alta disponibilidad y calidad de servicio por medio de una infraestructura de red que soporte grandes cantidades de tráfico, además de poseer escalabilidad y flexibilidad.

Mediante la realización del levantamiento y análisis de información de la situación actual de red, con su topología y elementos constituyentes es posible tener una idea clara de su estado actual, para lo cual se debe tener en cuenta aspectos claves como: cableado estructurado, estructura física y lógica de la red, cantidad de usuarios y su función dentro de cada departamento, ubicación y estado de puntos de red, comportamiento del espectro electromagnético dentro de las instalaciones, además de los elementos que conforman la parte activa de la red.

### **3.2 LEVANTAMIENTO DE INFORMACIÓN**

Las instalaciones de la institución tienen aproximadamente un uso de 1 año a partir de su construcción. Cabe señalar que el proyecto original no

contemplaba un proyecto de VOZ Y DATOS el mismo que fue concebido de manera básica y a lo largo de su vida útil la edificación ha sufrido cambios a nivel internos afectando esto a su estructura de red; así también la masificación del uso de las TIC ha obligado a la infraestructura de red presente a adaptarse a los requerimientos, demandando nuevos puntos de red para la prestación del servicio.

Sin embargo debido a que en sus inicios no se consideró tal crecimiento ni el uso masivo de nuevas tecnologías de información, hace necesario que se realice un estudio que permita identificar el estado actual de la red y sus requerimientos en cuanto a servicios y seguridad de la misma. Para esto es necesario comenzar con un levantamiento de información, el cual muestre las características propias de la red y brinde una idea clara de su estructura, teniendo en cuenta además que al momento no existe documentación actualizada de la misma.

### 3.2.1 DISTRIBUCION Y UBICACIÓN FISICA DE LOS PUNTOS

Fuente: (Ministerio Del Deporte Ecuador, 2014)

<b>ADMINISTRATIVO</b>	<b>VOZ</b>	<b>DATOS</b>
<b>1ER PISO CENTRO MEDICO</b>		
FISIOLOGIA	1	1
SALA DE ESPERA INFORMACION	1	1
ENFERMERIA	1	1
CONSULTORIO	1	1
CONSULTORIO	1	1
ODONTOLOGIA	1	1
ACCESS POINT PB		1
<b>2DO PISO ADMINISTRATIVO</b>		
OFICINA DE LOGISTICA	2	2
OFICINA DE METODOLOGIA	2	2
PAGADURIA	2	2
CONTABILIDAD	4	4
SECRETARIA	1	1
CUARTO DE CONTROL	1	1
ADMINISTRACION 1	1	1
ADMINISTRACION 2	1	1
SALA DE JUNTAS	1	1
SERVICIO SOCIAL	2	2
OFICINA DE ESTADISTICA	2	2
OFICINA DE EVALUACION FUNCIONAL DEPORTIVA	2	2
Total:	30	31

.2.- CANCELES Y VESTIDORES: Baños y área de vestidores

- 3.- COLISEO DE USO MULTIPLE: Cancha deportiva con graderíos, camerinos, baños, en tres niveles de plantas, parqueadero.

<b>COLISEO DE USO MULTIPLE</b>	<b>VOZ</b>	<b>DATOS</b>
ACCESS POINT GRADERIOS		2
CABINAS DE TRANSMISION	2	2

- 6.- GIMNASIO DE POTENCIACION: Cuadrilátero de box y 2 gimnasios oficina entrenadores.

<b>GIMNASIO DE POTENCIACION</b>	<b>VOZ</b>	<b>DATOS</b>
OFICINA	1	1

- UNIDAD EDUCATIVA:
  - 7.- BLOQUE 1: Aulas, Laboratorio, Oficinas, en 2 plantas
  - 8.- BLOQUE 2: Aulas y Oficinas en 2 plantas
  - 9.- BLOQUE 3: Aulas , Biblioteca, Laboratorio, en 2 plantas

<b>BLOQUE EDUCATIVO</b>	<b>VOZ</b>	<b>DATOS</b>
<b>LABORATORIOS</b>		
SALA DE PROFESORES	4	4
ADMINISTRACION	5	5
AULA DE COMPUTACION	1	25
<b>AULAS</b>		
SALA DE PROFESORES	4	4
ADMINISTRACION	5	5
ACCESS POINT PB		1
<b>BIBLIOTECA</b>		
ESTUDIOS DIRIGIDOS 2	1	1
ESTUDIOS DIRIGIDOS 2	1	1
ESTUDIOS DIRIGIDOS 3	1	1
ESTUDIOS DIRIGIDOS 4	1	1
LABORATORIO DE INTERNET		35
	23	83

- 10.- BATERIA SANITARIA
- 11.- CAMERINOS PISTA ATLETICA: camerinos y baños
- 14.- COLISEO DE CONTACTO: 2 Rings, camerinos y baños
- 15.- RESIDENCIA: Dormitorios en 2 plantas y piscina

<b>RESIDENCIA</b>	<b>VOZ</b>	<b>DATOS</b>
ACCESS POINT PLANTA BAJA		2
ACCESS POINT PLANTA ALTA		2

- 16.- SERVICIOS COMPLEMENTARIOS: Dormitorios, auditorio, área de lavado y planchado

<b>SERVICIOS COMPLEMENTARIOS DE RESIDENCIA</b>	<b>VOZ</b>	<b>DATOS</b>
RECEPCION	2	2
ADMINISTRACION	1	1
SECRETARIA	1	1
AUDITORIO	1	1

- 17.- RESTAURANTE: Comedor, Área de preparación de alimentos, bodegas y cuartos fríos.

<b>RESTAURANTE</b>	<b>VOZ</b>	<b>DATOS</b>
OFICINA	1	1
ACCESS POINT RESTAURANTE	1	1

- 18.- BLOQUE RECREACIONAL: Sala de juegos, cocina y comedor

<b>BLOQUE RECREACIONAL</b>	<b>VOZ</b>	<b>DATOS</b>
SALON RECREACIONAL	2	2
ACCESS POINT		2

- 19.- CAMERINOS FUTBOL SINTETICO: camerinos y baños
- 22.- CAMERINOS BEISBOL: camerinos y baños
- AREAS VERDES: plazoletas, canchas abiertas, camino periférico.

#### **RESUMEN:**

<b>BLOQUE</b>	<b>PTOS DE DATOS</b>
BLOQUE CENTRO MEDICO	10
BLOQUE ADMINISTRATIVO	24
COLISEO DE USO MULTIPLE	4
GIMNASIO DE POTENCIACION	1
BLOQUE EDUCATIVO	83
BLOQUE RESIDENCIA	4
SERVICIOS COMPLEMENTARIOS DE RESIDENCIA	6
RESTAURANTE	2
BLOQUE RECREACIONAL	4
<b>TOTAL</b>	<b>128</b>

### **3.2.2 CABLEADO ESTRUCTURADO**

El cableado estructurado de cualquier institución constituye la base fundamental para la prestación de servicios de red, por lo cual es importante que este se encuentre en perfecto estado. Dentro del levantamiento de información del cableado estructurado se han considerado los siguientes elementos: cableado horizontal, cableado vertical, área de trabajo, cuarto de telecomunicaciones y cuarto de equipos, cuarto de entrada de servicios y sistema de puesta a tierra.

#### **3.2.2.1 Subsistema Horizontal**

- El cableado horizontal del complejo es par trenzado categoría 5e, para su distribución cada uno de los bloques del edificio cuentan con su respectivo cuarto de telecomunicaciones y bandejas metálicas de distribución.
- Desde las bandejas de distribución metálicas del cableado horizontal hacia las localizaciones de salida del cableado estructurado se utiliza tubo conduit, el cual no soporta nuevas conexiones. Las canalizaciones no sobrepasan los 6 metros en su trayectoria.
- Los conectores, terminaciones y patch cord utilizados son cable UTP categoría 5e.
- En algunos casos para la salida de los puntos de red se utiliza los ductos del interior de los modulares.

- Debido a la demanda de puntos de red se han realizado un mínimo de nuevas instalaciones de cableado par trenzado categoría 5e.

#### **3.2.2.1.1 Certificación de puntos de red**

La infraestructura de cableado estructurado actual con la que cuenta el complejo Deportivo tiene un tiempo de uso aproximado de 1 años, por lo cual, es necesario realizar la certificación del cableado estructurado con el equipamiento adecuado de todos los puntos de red, para conocer su estado y rendimiento.

Para la certificación se utilizó los equipos certificadores de red Fluke Network con los cuales se determinó el cumplimiento o no de los parámetros de red, permitiendo así determinar también el cumplimiento de las normas y estándares de cableado estructurado basados en el TSB. *Ver 1.8.5 Normas y Estándares de CE vigentes.*

Los parámetros a considerar para la certificación del cableado estructurado del complejo se basan en el boletín técnico TSB , los mismos que se detallan a continuación:

- Mapa de Cableado
- Longitud del Cableado
- Pérdida de inserción
- Pérdida de Retorno
- Pérdida de Paradiafonía NEXT

- Pérdida de Paradiafonía por Suma de Potencia (PSNEXT)
- Pérdida de Paradiafonía en el Extremo Lejano por Igualación de Nivel (ELFEXT)
- Pérdida de Paradiafonía en el Extremo Lejano por Igualación de Nivel y Suma de Potencia (PSELFEXT)
- Retardo en la Propagación
- ACR

La certificación de los puntos de red se pueden resumir en “**Pasa**” o “**No Pasa**”, para que los puntos de red pasen la certificación deben cumplir con todos los valores mínimos de los diferentes parámetros medidos. Si uno o más parámetros no cumplen con los valores umbrales mínimos definidos para cada valor, el punto de red no pasará la prueba realizada. Los resultados de las pruebas realizadas se tratan dentro del análisis de información recopilada durante este proceso.

## Principales características del equipamiento utilizado.

### DTX-1800 Cable Analyzer Fluke Network [62]

El DTX Cable Analyzer Series de Fluke Network es una plataforma de certificación para cableado de redes, dentro de sus principales características están:

- Tiempo de comprobación automática menor a 9 segundos.
- Ancho de Banda máximo de 900MHz.
- Almacenamiento de datos gráficos de los resultados.
- Interfaces USB /Serie.
- Adaptador de enlace permanente.
- Adaptador de canal.
- Integración de módulos de fibra óptica.
- Intercomunicación entre unidades principal y remota.





**Figura 6 Características Fluke Network DTX-1800**

Fuente (Fluke Co., 2010)

Linkware – Fluke Network (Fluke Co., 2010)

Software para gestión de pruebas de cableado. Permite gestionar y elaborar informes de los datos de las certificaciones de la infraestructura de cableado estructurado. Con la ayuda del software se permite descargar las pruebas realizadas y emitir los informes de las mismas. La versión utilizada es 1.4.

Cable ID	Date / Time	Length(m)	Summary	Headroom	Info	Test Link
1	10/21/2008 10:09:39am	146	PASS	Null		General Fiber
2	10/21/2008 10:21:56am	147	PASS	Null		General Fiber
3	10/24/2008 09:10:15pm	43	PASS	2.36 (cm)		10GBASE-S
4	10/24/2008 09:10:15pm	63	PASS	2.79 (cm)		10GBASE-S
5	10/24/2008 09:35:24pm	512	PASS	Null		General Fiber
6	10/24/2008 09:45:54pm	148	PASS	Null		General Fiber
7	10/24/2008 09:12:11pm	201	PASS	Null		General Fiber
8	10/26/2008 04:09:13pm	43	PASS	2.36 (cm)		10GBASE-S
9	10/26/2008 04:09:13pm	63	PASS	2.49 (cm)		10GBASE-S
10	10/26/2008 04:37:28pm	144	PASS	2.44 (cm)		10GBASE-S
11	10/26/2008 04:37:29pm	64	PASS	2.44 (cm)		10GBASE-S
12	10/26/2008 04:34:13pm	64	PASS	2.28 (cm)		10GBASE-S
13	10/26/2008 04:34:13pm	64	PASS	2.40 (cm)		10GBASE-S
14	10/26/2008 10:36:25am	45	PASS	3.5 (dB-7)		Tel. Car 6 Prem. Link
15	12/16/2010 08:24:06pm	63	PASS	5.9 (dB-7)		Tel. Car 6A Channel
16	12/16/2010 11:44:42am	43	PASS	5.7 (dB-7)		Tel. Car 6A Channel
17	12/16/2010 12:01:47pm	40	PASS	6.1 (dB-7)		Tel. Car 6 Prem. Link

Test Link: General Fiber  
Cable Type: Multimode 50

**Figura 7. Software LinkWare - Fluke Network (Fluke Co., 2010)**

Fuente (Fluke Co., 2010)

### **3.2.2.2 Subsistema Vertical**

El cableado vertical del complejo se encuentra conectado a través de fibra óptica multimodo FC, excepto dos de los bloques del edificio y el enlace utilizado para la conexión hacia el switch de la red wireless, los cuales se encuentran conectados con cable par trenzado UTP categoría 5e.

Los enlaces de fibra óptica se encuentran instalados utilizando ductos subterráneos unidos a los ductos que llegan a los cuartos de telecomunicaciones; de igual manera se encuentran instalados los enlaces de cable UTP.

El cuarto de control se encuentra ubicado en el segundo piso del edificio administrativo.

De ese lugar se realiza la distribución para los siguientes bloques a través de fibra óptica:

Bloque Educativo Laboratorios.

Bloque Educativo Aulas.

Bloque Educativo Biblioteca.

Gimnasio de Potenciación.

Cocina Restaurante.

Bloque recreacional.

### **3.2.2.3 Área de trabajo**

Las tomas utilizadas como salidas en las áreas de trabajo para conexión del equipo de usuario hacia la toma de conectorización, son salidas dobles que utilizan jack modulares Cat 5e.

La asignación de los pines de los jack modulares se han definido como base en la norma T568B.

### **3.2.2.4 Cuartos de Telecomunicaciones**

En el edificio administrativo se encuentra el Cuarto de Telecomunicaciones central.

Existen rack de piso en los bloques:

Administrativo.

Bloque educativo aulas.

Bloque educativo Laboratorios.

Bloque educativo Biblioteca.

Existen Racks de pared en los bloques:

Gimnasio de potenciación.

Servicios complementarios de Residencia.

Bloque recreacional.

Coliseo.

Cada rack cuenta con patch panels de datos y de voz, además de ODFs59 para la conectorización del backbone de Fibra Óptica y switches de acceso marca HP V1910AL.

Hacia los cuartos de telecomunicaciones llegan ductos pertenecientes al sistema de ventilación del edificio.

Dentro de los cuartos de telecomunicaciones se encuentran instaladas cajas eléctricas de tensión para la alimentación de los sistemas de seguridad.

El ingreso a los cuartos de telecomunicaciones se encuentra restringido al personal de administradores de red del edificio.

Las luminarias presentes en los cuartos de telecomunicaciones son lámparas fluorescentes.

Al interior de los cuartos de telecomunicaciones no existen lámparas de emergencia ni indicativos de salidas de emergencia.

### **3.2.2.5 Data Center**

En el Data Center se encuentran tres racks de piso tipo gabinete los mismos que albergan tanto al equipamiento activo como los servidores de aplicaciones del edificio.

PRIMER RACK: DATOS.

SEGUNDO RACK: VOZ.

TERCER RACK: PERIFONICA Y SISTEMA DE CAMARAS DE SEGURIDAD.

**Tabla 3. Lista de servidores con sus respectivas IP**

SERVIDOR	n
Servidor de Base de Datos	N/d

**Fuente: Javier Espinosa**

**Tabla 4. Lista de equipamiento activo con su respectiva IP**

Equipamiento Activo	IP
Switch 3com serie 7700	192.168.0.245/24

**Fuente: Javier Espinosa**

En el primer rack el router de WAN que es el equipo Router Cisco 881 el cual da la conectividad con CNT de un enlace de 2Mb a través de fibra óptica, llega a un conversor de fibra a cobre e ingresa al router. El router da conectividad al equipo 3Com 5500 el cual es un switch con conexión de fibra a través del cual se conectan los diferentes bloques a través de un enlace interno de fibra óptica.

- El único servidor del complejo se encuentran físicamente en el primer rack del Data Center; sus enlaces de conexión llegan hacia el switch de distribución.
- Todo el equipamiento activo y servidor se encuentran conectados al sistema eléctrico regulado.
- El Data Center cuenta con un sistema de enfriamiento que controla la temperatura del mismo manteniéndola entre los 20°C y 23°C; además

se cuenta con conexión a UPS de 80kVA los cuales protegen a la red en caso de fallas de energía.

- Todo el backbone vertical del complejo es manejado desde el Data Center.
- El Data Center cuenta con sensores de humo para detectar posibles peligros de fuego.
- El Data Center se encuentra custodiado por el personal de seguridad del edificio, además se cuenta con mecanismos de seguridad física (tarjetas magnéticas) asegurando que solo el personal autorizado ingrese al mismo.

#### **3.2.2.6 Sistema de Puesta a Tierra**

- El edificio cuenta con un sistema de puesta a tierra tipo malla.

### **3.2.3 ELEMENTOS DE PARTE ACTIVA**

- Entre los elementos que conforman la parte activa se tienen: equipos de red y equipos de control de acceso y seguridad:

#### **3.2.3.1 Equipos de RED**

- Dentro de los equipos de red con los que cuenta la institución se tienen equipos en funcionamiento y equipos fuera de servicio, como se enumeran a continuación:

**Tabla 5. Listado del equipamiento**

CANTIDAD	MARCA	MODELO SERIE	ESTADO
1	Router Cisco	881	OPERATIVO
1	Switch 3Com	7700	OPERATIVO
8	Switch 3Com	5500	OPERATIVO
1	Switch HP	2910 al	EMPACADO
1	Switch HP	1910 24G	EMPACADO
3	Switch HP	1910 48G	EMPACADO
16	Access Point HP	V M200	OPERATIVO

**Fuente: Javier Espinosa**

Dentro del equipamiento activo en estado operativo detallado en la tabla 10, se puede indicar lo siguiente:

- El equipo que maneja los equipos de acceso y servidores de aplicaciones es un switch marca 3Com serie 7700, este además maneja 2 enlaces de conexión pertenecientes a los administradores de red.
- A nivel de la red interna de la institución se utilizan 8 switches serie 5500 los cuales dan servicio a toda la red cableada.
- Para el servicio de red inalámbrica se cuenta con 16 Access Point marca HP ubicados en el Bloque administrativo, bloque educativo, bloque recreacional, restaurante, bloque residencia.

## PRINCIPALES CARACTERÍSTICAS DEL EQUIPAMIENTO UTILIZADO.

(Cisco Co., 205)



**Figura 8. Router Cisco serie 800**

**Fuente:** (Cisco Co., 205)

- **Tipo de dispositivo:** Encaminador + conmutador de 4 puertos (integrado).
- **Factor de forma:** Externo.
- **Dimensiones (Ancho x Profundidad x Altura):** 32.5 cm x 24.9 cm x 4.4 cm.
- **Memoria RAM:** 256 MB (instalados) / 768 MB (máx.).
- **Memoria Flash:** 128 MB.
- **Protocolo de direccionamiento:** OSPF, RIP-1, RIP-2, BGP, EIGRP, HSRP, VRRP, NHRP, GRE.
- **Protocolo de interconexión de datos:** Ethernet, Fast Ethernet.
- **Red / Protocolo de transporte:** L2TP, IPSec.
- **Protocolo de gestión remota:** Telnet, SNMP 3, HTTP, HTTPS, SSH.
- **Características:**

Cisco IOS Advanced IP services, Soporte de NAT, Puerto de estado de interrupción (ISP), Soporte VLAN, Señal ascendente automática (MDI/MDI-X

automático), Snooping IGMP, Stateful Packet Inspection (SPI), filtrado de contenido, filtrado de dirección MAC, Soporte IPv6, Stateful Failover, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Fair Queuing (WFQ), Soporte de Access Control List (ACL), Quality of Service (QoS), Dynamic Multipoint VPN (DMVPN), Servidor DHCP, Virtual Route Forwarding-Lite (VRF-Lite), DNS proxy.

- **Cumplimiento de normas:** IEEE 802.1D, IEEE 802.1Q, IEEE 802.1x.

- **Alimentación:** CA 120/230 V ( 50/60 Hz ).

### Switch 3com serie 7700 (3Com, 2013)

Dentro de las principales características del switch marca 3com serie 7700 están:



**Figura 9. Switch 3Com serie 7700**  
Fuente: (3Com, 2013)

Dentro de las principales características del switch marca 3com serie 7700 están:

- Soporte de Switching 10-Gigabit, Gigabit, y Fast Ethernet, multicapa y de alto rendimiento.
- Soporte de capa 2: Direcciones MAC61 de 32K, 4096 VLANs, STP62, RSTP63 y MSTP64.
- Soporte de capa 3: Entradas de routing IP de 64k, OSPF, RIPv1/v2, PIM SM/DM65, IPX66.
- Soporte de PoE.
- Plataforma de chasis integrada.
- Rendimiento de 96 Gbps.

- Ancho de banda de 240 Gbps con rendimiento del sistema de 179 Mpps.
- Capacidad de backplane de hasta 96 Gbps.
- Soporte de switching local en módulos.
- Soporte de tramas jumbo (hasta 9KB).
- Soporta módulos 10Gigabit IEEE 802.3ae para conexiones de alta velocidad entre switches.
- Soporte de login de Red.

**Switch 3com serie 5500 (3Com, 2013)**



**Figura 10. Switch 3Com serie 5500**  
Fuente: (3Com, 2013)

- Switches de Capa 2/3/4 Fast Ethernet y Gigabit Ethernet.
- Funcionamiento multi-capa con rutas estáticas, RIP, OSPF, y PIM-DM y PIM-SM.
- Soporte de STP, RSTP, MSTP .
- Capacidad de apilamiento XRN68, hasta 8 unidades.
- Soporte de QoS69 y filtrado dependiente de las aplicaciones.
- Soporte de PoE70.
- Capacidad de switching de hasta 12,8 Gbps.

- Velocidad de transmisión de hasta 9,5 Mbps.
- Ancho de banda de apilamiento de 48 Gbps (96 Gbps full-duplex).
- Manejo de listas de control de acceso (ACLs).
- Autenticación basada en usuario.
- Soporte de encriptación DES71 de 56 ó 168 bits.
- Identificación de usuarios RADIUS.
- Autenticación PAP72/CHAP73/EAPoL74 (EAP sobre LAN).
- Filtrado de paquetes.
- Encriptación SNMP v3.
- Soporte de login de red IEEE 802.1X.
- Soporte de autenticación, auto-iniciación de VLAN y perfiles de QoS.
- Privilegios de acceso multinivel.

**HP 1910-24G(JE006A)** (Hp Hewlet Packard, 2013)



**Figura 11. HP 1910-24G**

**Fuente:** (Hp Hewlet Packard, 2013)

Los conmutadores HP 1910 son conmutadores Gigabit y Fast Ethernet de configuración fija con gestión inteligente, diseñados para empresas pequeñas en una solución fácil de administrar. La serie tiene 8 modelos Gigabit y 5 Fast Ethernet.

Los modelos gigabit son los siguientes: modelos no PoE 10/100/1000 de 8, 16, 24 y 48 puertos; Y dos modelos PoE 10/100/1000 de 8 puertos y dos de 24 puertos. Los modelos Gigabit tienen puertos SFP Gigabit adicionales verdaderos para la conectividad por fibra.

Los modelos Fast Ethernet son: 8-, 24 y 48 modelos 10/100 no PoE y 8, 24 modelos 10/100 PoE+.

Los modelos con Fast Ethernet vienen con 2 puertos de enlaces ascendentes combinados adicionales. Todos los modelos HP 1910 admiten montaje en bastidor o funcionamiento en formato escritorio.

Las funciones personalizables incluyen funciones de capa 2 básica como VLAN y agregación de enlaces, así como funciones avanzadas como enrutamiento estático de Capa 3, IPv6, ACLs y protocolos de árbol de expansión. Los conmutadores HP 1910 vienen con una garantía de por vida que cubre la unidad, los ventiladores y las fuentes de alimentación.

## **Gestión**

Administración web sencilla: con una interfaz gráfica del usuario Web e intuitiva, permite una gestión fácil del conmutador, incluso por parte de usuarios que no tengan muchos conocimientos técnicos compatible con http y http seguro (https).

Administración de IP sencilla: permite la gestión de hasta cuatro dispositivos HP 1910 mediante una única interfaz web; simplifica la administración de varios dispositivos.

GUI Web segura: ofrece una interfaz gráfica de usuario fácil de usar y segura para la configuración del módulo mediante HTTPS.

SNMPv1, v2c y v3: facilita la gestión del conmutador, ya que el dispositivo puede ser detectado y supervisado desde una estación de gestión SNMP.

Registro completo de sesiones: proporciona información detallada para la identificación y solución de problemas.

### **Calidad de servicio (QoS)**

Control de transmisión: permite limitar la velocidad de tráfico de transmisión para reducir el tráfico de transmisión no deseado en la red.

Limitación de la tasa: máximos obligatorios según ingresos por puerto y mínimos por puerto y por cola.

Asignación de prioridades de tráfico: proporciona paquetes sensibles al tiempo (como VoIP y vídeo) con prioridad respecto a otros tráficos basados en DSCP o clasificación IEEE 802.1p DSCP; los paquetes se asignan a cuatro colas de hardware para obtener un rendimiento más efectivo.

### **Conectividad**

IPv6: Host IPv6: permite que los conmutadores se administren y desplieguen en el perímetro de la red IPv6. Enrutamiento IPv6: admite rutas

estáticas IPv6. Búsqueda de MLD: direcciona el tráfico de multidifusión IPv6 a la interfaz apropiada, evitando que el tráfico se sature. IPv6 ACL/QoS: admite ACL y QoS para el tráfico de red IPv6.

MDI/MDIX automático: se ajusta automáticamente para cables normales o cruzados en todos los puertos 10/100/1000.

Control de flujo IEEE 802.3X: brinda un mecanismo de limitación de flujo propagado a través de la red, el cual evita la pérdida de paquetes en los nodos congestionados

Listo para la alimentación a través de Ethernet (PoE) IEEE 802.3af: proporciona hasta 15,4 W por puerto para alimentar teléfonos IP compatibles con la normativa, puntos de acceso inalámbrico, cámaras Web y otros (todos los modelos PoE).

IEEE 802.3at Alimentación a través de Ethernet (PoE+): proporcione hasta 30 vatios por puerto, lo que permite la compatibilidad con los últimos dispositivos PoE+, como teléfonos IP, puntos de acceso inalámbrico y cámaras de seguridad, además de cualquier dispositivo final que cumpla con IEEE 802.3af; elimine el costo de cableado eléctrico adicional y circuitos que de otra forma serían necesarios en implementaciones de teléfonos IP y WLAN. (Nota: se aplica a todos los modelos PoE, salvo los dos modelos 24G-PoE que admiten una implementación de PoE+ pre-estándar).

## Seguridad

Listas de control de acceso (ACL) avanzadas: Permite filtrar el tráfico de red y mejora la red mediante las ACLs basadas en MAC e IP; las ACLs basadas en tiempo permiten una mayor flexibilidad en la gestión del acceso a la red.

Secure Sockets Layer (SSL): cifra todo el tráfico HTTP, permitiendo un acceso seguro a la interfaz gráfica de usuario de administración basada en navegador del conmutador.

Inicios de sesión en redes IEEE 802.1X y RADIUS: controla el acceso por puerto para la autenticación de usuarios y el proceso de responsabilidades.

Asignación automática de VLAN: asigna automáticamente usuarios a la VLAN apropiada según su identidad, ubicación y hora del día.

Protección de puertos STP BPDU: bloquea las Bridge Protocol Data Units (BPDUs) en los puertos que no necesitan BPDUs, evitando ataques de BPDUs falsas.

### SWITCH HP CORE MODELO : 2910aI-24G L3 - L4



**Figura 12. Switch 3Com serie 7700**  
**Fuente:** (Hp Hewlet Packard, 2013)

Switch - 20 Puertos 10/100/1000 + 4 Puertos Dual Personality (10/100/1000 SFP).

Soporta hasta 4 Puertos 10G adicionando módulo Layer 2,3 y 4 .

Administración :

- HP ProCurve Manager Plus
- IEEE 802.1p QoS
- IEEE 802.1q VLAN
- HTTP
- CLI
- Telnet
- DHCP
- SNMP v1, v2c, v3
- RMON 1, 2, 3, 9

Puertos : 20 autosensing 10/100/1000 (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T).

- Media Type: Auto-MDIX, Duplex: 10BASE-T/100BASE-TX: half o full; 1000BASE-T: full only; 4 Puertos dual-personality, cada puerto puede ser usado como RJ-45 10/100/1000 (IEEE 802.3 Type 10Base-T; IEEE 802.3u Type 100Base-TX; IEEE 802.3ab 1000Base-T Gigabit Ethernet) o como mini-GBIC slot (Usado por mini-GBIC transceivers); 1 Puerto Serial de Consola RJ-45; Soporta maximo 4 Puertos 10-GbE ports, con modulo opcional.

### Access Point HP M200 802.11



**Figura 13. Access Point HP M200**

**Fuente:** (Hp Hewlet Packard, 2013)

El punto de acceso 802.11n HP M200 proporciona conectividad inalámbrica para su red ampliable. Aprovechese totalmente del estándar IEEE 802.11n de próxima generación con la capacidad de doble banda del punto de acceso M200, mientras admite simultáneamente dispositivos IEEE 802.11a o 802.11b/g.

La nueva interfaz de usuario de Web hace el punto de acceso M200 fácil de configurar y todavía retiene funcionalidad clave, para mantener sus datos importantes seguros.

#### **Gestión**

Interfaz de usuario de Web segura y fácil de usar: Página de instalación rápida: consolida la configuración clave en una página para configuración

sencilla y rápida para escenarios de implementación comunes. Sesiones de gestión segura HTTPS: evitan que las sesiones de gestión sean observadas en la red.

Integración con HP PCM: permite la detección y correlación mediante HP PCM, que se puede descargar gratuitamente en Internet; proporciona todas las herramientas básicas necesarias para administrar una red de forma efectiva, además de una versión de prueba de 60 días de HP PCM+.

Protocolo de detección de capa de enlace (LLDP) IEEE 802.1AB: protocolo de detección automatizada de dispositivos que facilita la asignación por parte de las aplicaciones de administración de red.

Niveles de privilegios de operador y administrador: proporciona niveles de acceso de sólo lectura (operador) y lectura-escritura (administrador) para la gestión de Web.

## **Conectividad**

Punto de acceso de doble banda totalmente compatible con IEEE 802.11n: Soporte de banda de frecuencia de 2,4 GHz: utiliza sus clientes inalámbricos IEEE 802.11n junto a dispositivos heredados IEEE 802.11b/g. Soporte de banda de frecuencia de 5 GHz: opera sus dispositivos IEEE 802.11n y 802.11a en el espectro de 5 GHz, lo que tiene menos interferencia de los hornos microondas, dispositivos Bluetooth® y teléfonos inalámbricos.

Opción de dispositivo alimentado por IEEE 802.3af PoE (PD): simplifica la implantación y reduce espectacularmente los costos de instalación al

eliminar los costos y el tiempo que supone el suministro de alimentación eléctrica local a cada ubicación de punto de acceso.

MDIX automático: se ajusta automáticamente para cables normales o cruzados en los puertos 10/100/1000.

Protocolo de árbol de expansión (IEEE 802.1D): evita los bucles de red.

## **Movilidad**

Cuatro comunidades inalámbricas: consolida la calidad de servicio, seguridad y configuración VLAN en un identificador fácil de gestionar por SSID.

Segmentación de clase de servicio: Hasta cuatro SSIDs (uno por comunidad inalámbrica): permite al administrador identificar varios conjuntos de servicios para que los clientes accedan. Hasta cuatro VLANs (uno por comunidad inalámbrica): El etiquetado VLAN IEEE 802.1Q proporciona seguridad entre los grupos de trabajo. Priorización basada en comunidad inalámbrica: permite al administrador asegurar que el tráfico de red clave es priorizado, ponderando comunidades inalámbricas específicas.

Selección automática de canales (ACS): ayuda a reducir las interferencias entre canales al seleccionar automáticamente un canal de radio sin ocupar.

Modos de sistema de distribución inalámbrica (WDS): Punto de acceso y puente WDS, punto de acceso sólo, puente WDS sólo y monitor: permite a los puntos de acceso HP V-M200 802.11n conectarse de forma inalámbrica

con otros puntos de acceso HP V-M200 802.11n sin una red troncal cableada; esto es útil para ampliar la red a través de áreas donde no existe infraestructura cableada.

Interoperabilidad: cumple con las certificaciones de Wi-Fi Alliance, incluyendo IEEE 802.11n Wi-Fi y WPA2, para garantizar la interoperabilidad entre varios proveedores.

## **Seguridad**

Funciones de control de acceso de cliente AP: - Autenticación IEEE 802.1X mediante EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP. - Autenticación de dirección MAC mediante el uso de listas de acceso locales o RADIUS. - RADIUS AAA mediante EAP-MD5, PAP, CHAP y MS-CHAPv2. - Aislamiento de cliente inalámbrico de capa 2.

Autenticación MAC basada en RADIUS: el cliente inalámbrico se autentica con un servidor RADIUS según la dirección MAC del cliente; esto resulta práctico para clientes sin interfaz de usuario o con una interfaz mínima.

Opción de IEEE 802.11i, WPA2 o WPA: bloquea el acceso inalámbrico no autorizado al autenticar a los usuarios antes de conceder el acceso a la red; el Estándar de cifrado avanzado (AES) o Protocolo de integridad de clave temporal (TKIP) garantiza la integridad de los datos del tráfico inalámbrico.

Secure Sockets Layer (SSL): cifra todo el tráfico HTTP, permitiendo un acceso seguro a la interfaz de gestión basada en navegador de Web del punto de acceso.

Filtro del tráfico del cliente de puente inalámbrico local: cuando está activado, evita la comunicación entre dispositivos inalámbricos asociados con el mismo punto de acceso.

### **LECTOR DE HUELLAS DIGITALES AR-821 E/F**

Controlador de acceso con lector de “HUELLA DIGITAL”, además tiene Lector de proximidad incorporado y teclado para ser programado de forma independiente (sin software).

Este equipo puede funcionar con software, para control de acceso con registro, para control solo de asistencia o sin software como control de acceso Stand Alone ( abre puertas sin registro).

Su PANTALLA LCD, muestra la fecha, hora, código de tarjeta De proximidad ( ya sea autorizada o no ), (Pin Ok o error Pin), Huella incorrecta o autorizada, todo el menú de su programación y el nombre y apellido del Usuario (11 caracteres como máximo).

Fuente de alimentación: 12VDC

Consumo de corriente : 150mA en Stand By 190mA en Lectura

Modos de comunicación

*Comunicación serial*

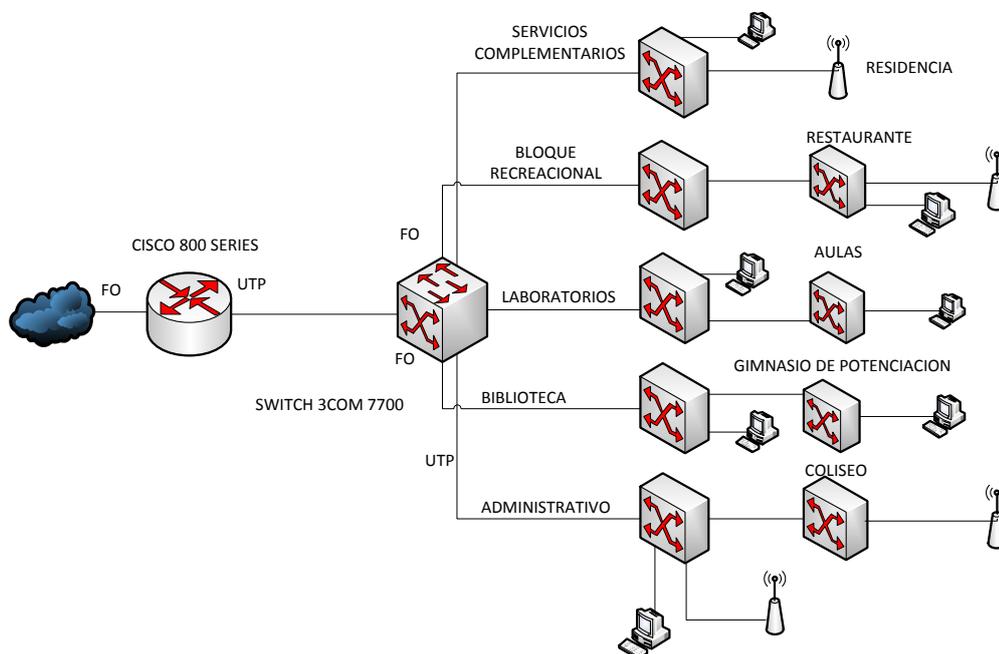
Mediante el conversor de RS-485 a USB (AR-321CM)

Mediante el módulo conversor de RS-485 a TCP/IP (AR- 727CM)

### 3.2.4 ESQUEMA DE LA TOPOLOGÍA DE RED ACTUAL

#### 3.2.4.1 Topología Física

La red interna desde donde se proveen servicios de conectividad para los usuarios de la institución y acceso al servidor de respaldo, su topología física se muestra en la figura.



**Figura 14. Topología Física**

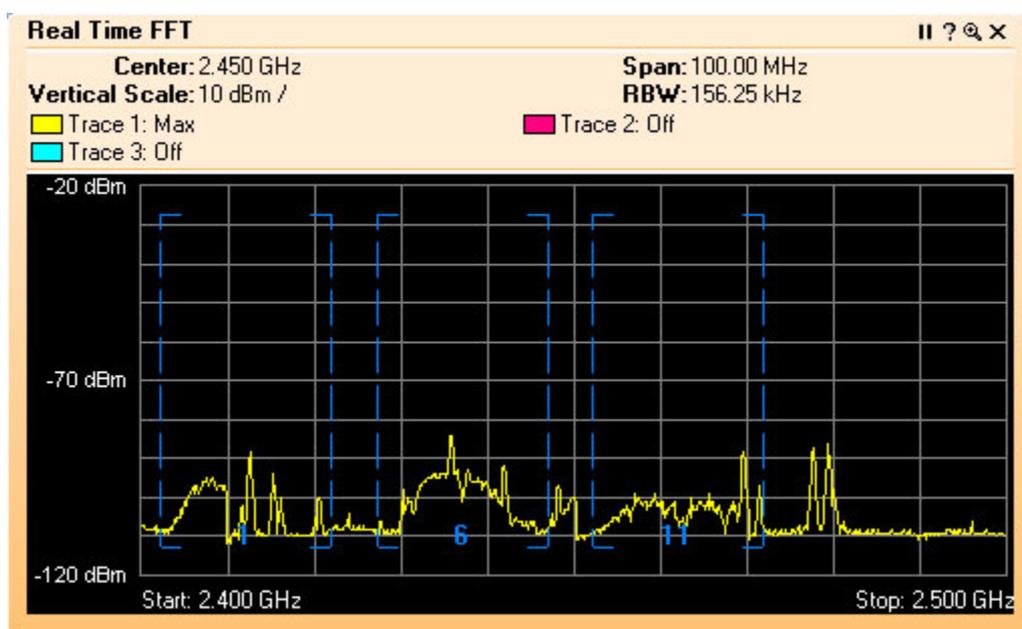
**Fuente:** Javier Espinosa

#### 3.2.4.2 Topología Lógica

La topología lógica de la red se encuentra establecida en base a un direccionamiento IP para cada uno de los equipos de la institución. Actualmente no se han creado VLAN por lo que más adelante se va a recomendar su creación.

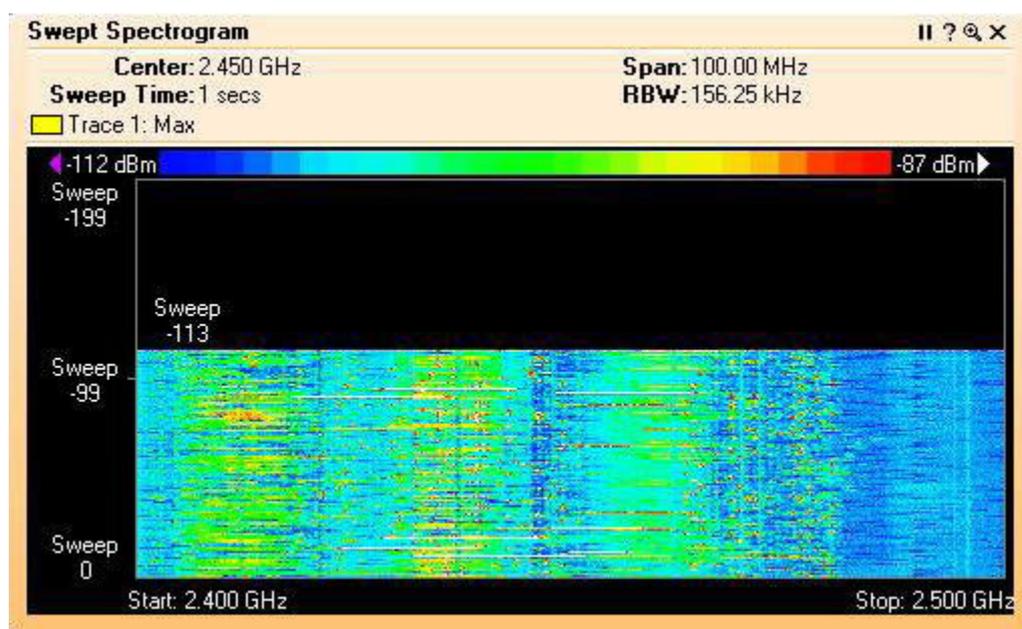
### 3.2.5 ESPECTRO WIFI

El análisis del espectro electromagnético realizado con AirMagnetSpectrum XT dentro del área de estudio muestra que se encuentran operando los canales 1, 6 y 11 a las frecuencias 2412 MHz, 2437 MHz, 2462 MHz respectivamente. En la figura 34 se aprecian los canales en tiempo real con las respectivas potencias captadas en un promedio de -100 dBm.



**Figura 15. FFT en tiempo real**  
**Fuente:** Equipo de Prueba AirMagnetSpectrum XT

En la figura 3.11 se observa el barrido espectral y la utilización de las frecuencias en dBm. El color verde de la figura muestra la utilización de los canales, mientras que el color azul muestra la disponibilidad del espectro.



**Figura 16. Barrido del espectro**

**Fuente:** Equipo de Prueba AirMagnetSpectrum XT

### **3.3 ANÁLISIS DE SITUACIÓN ACTUAL**

Con el levantamiento de información realizada es conveniente que se proceda a hacer el análisis de la misma, mediante la cual se permita detectar los puntos positivos y las falencias de la infraestructura actual de red.

#### **3.3.1 CABLEADO ESTRUCTURADO**

La infraestructura de red del edificio del Complejo Deportivo cuenta con 128 puntos de red activos, los cuales brindan conectividad a los usuarios hacia la red interna y red externa de la institución. Como parte del levantamiento realizado se actualizó la información referente a usuarios, funciones y perfiles asignados tanto para navegación como para Directorio Activo, complementado de esta manera la distribución de puntos de red; su detalle se muestra en el Anexo 1 “*Distribución de Puntos de Red*”.

### 3.3.1.1 Cableado Horizontal

- Es necesario que en su totalidad se separe la red de energía de la de datos para evitar causar problemas de interferencia electromagnética en los cables de datos. Además ni los cables de datos, ni los cables de energía eléctrica se encuentran debidamente organizados.
- Las canalizaciones realizadas con tubo conduit para la distribución del cableado horizontal hacia las salidas de usuario se encuentran saturadas; por lo cual estas canalizaciones no soportan adición de nuevos puntos de red.
- Los cables que van desde el rack hasta las bandejas de techo horizontal no se encuentran instalados con las debidas canalizaciones y accesorios, lo cual puede causar tensiones excesivas sobre el cableado instalado; además se podría sobrepasar los niveles de curvatura permitidos para los mismos, afectando también a la estética de dichos cuartos especialmente en el rack de pared de Servicios complementarios de Residencia.
- Existen puntos de red que tienen daños físicos como jacks sueltos, sin face plate, cajetines sueltos y cajetines rotos causantes de la disminución de puntos de red, problemas de conexión y/o reducción del performance de la misma.
- Existen puntos de red sin una debida etiquetación, lo cual dificulta su ubicación dentro del edificio; así también se pudo detectar que la etiquetación utilizada no es la más adecuada debido a que ésta no

permite tener una idea clara de su ubicación y servicio prestado a breve vista.

- Teniendo en cuenta que en un inicio el uso de los sistemas informáticos no estaba masificado, con el crecimiento de usuarios dentro de la red se ha debido realizar nuevas conexiones hacia los switches de bloque. Algunas de estas conexiones se conectan directamente hacia el switch del cuarto de telecomunicaciones sin que éstos lleguen a patch panel y sin usar ductos, ni canaletas en su instalación. Estos factores coadyuvan a la disminución del performance en la red, además de esta manera se dificulta la identificación de las conexiones en el cuarto de telecomunicaciones al no contar con un punto de control en la red, así también el orden en los mismos se ve afectado.

- 

### **3.3.1.2 Certificación de puntos de red**

Al ser la red relativamente nueva se tuvo acceso a la certificación de puntos de red realizada el año pasado se recomienda solicitar una nueva certificación y tener datos actuales para su evaluación. Para las pruebas desarrolladas se utilizó los certificadores de red Fluke Network, con los resultados obtenidos se realizó un análisis de la información recopilada con la ayuda del software de gestión LinkWare. Ver Anexo 3 “*Pruebas de Certificación*”.

### **3.3.1.2.1 Análisis de resultados**

- Luego de realizada la certificación de los puntos de red del complejo se tuvo como resultado que todos los puntos pasaron la certificación para cat 5e.

#### **Posibles causas de los problemas para la certificación de los cables de red.**

El **mapa de cableado** puede fallar por: cortes a lo largo del cable, cables mal ponchados, jacks sin face plate o cables de red sueltos (al estar los jack sueltos estos pueden sufrir daños debido a una mala manipulación, o pueden ser pisados o incluso rotos). El uso inapropiado de canaletas y conectores finales o simplemente el obviar la instalación de algunos de ellos son causantes de problemas con el mapa de cableado.

Las **pérdidas de retorno** pueden ser causadas por maltrato del cable durante su instalación, torceduras de los cables de red, curvaturas menores o iguales a 90 grados o el uso inapropiado de accesorios de cableado estructurado, además un factor influyente en el mismo es la longitud del enlace.

La **interferencia por extremo cercano** puede darse por el destrenzado del cable, cortes en el aislante de los pares, ruptura de los hilos del cable, altas frecuencias de trabajo, así como también influye la longitud del enlace. Además este factor se ve alterado por fuentes de interferencia electromagnética externas cercanas a los cables de datos (cajas eléctricas, motores, entre otros).

Del análisis de las pruebas de certificación, se deduce que la mayor parte del cableado estructurado del complejo se encuentra en buenas condiciones, por tanto el mismo puede seguir operando dado que al momento la red no demanda de mayores prestaciones, además teniendo en cuenta que los servicios que se ofrecen por la red son netamente de datos. Cabe destacar que debido a que no se cuenta con una firma autorizada que acredite las pruebas de certificación realizadas, las mismas constituyen un documento que si bien cumple con todos los requerimientos técnicos, éstos necesitan ser avalados por una institución autorizada para que sea considerado como un informe válido.

### **3.3.1.3 Cableado Vertical**

El backbone vertical que conecta los bloque principales del complejo es a travez de fibra óptica; solo la conexión hacia el coliseo y el restaurante es UTP Cat5.

El backbone instalado no cuenta con redundancia, por lo que si se produce un corte físico o cualquier otro daño a lo largo del backbone, se dejaría sin servicio a toda la red o parte de ella.

- La fibra óptica principal que llega a cada uno de los rack de telecomunicaciones de los bloques, no tiene ninguna protección, lo que la hace susceptible a daños físicos involuntarios o debido al mal manejo de la misma.

- En algunos de los departamentos las tomas de datos utilizadas como salidas en las áreas de trabajo no cuentan con la debida etiquetación, causando principalmente problemas para la administración del cableado estructurado del edificio.
- Ciertos face plates se encuentran sueltos o en mal estado, pudiendo ocasionar problemas en el mapa de cableado debido a la manipulación a la que se encuentran expuestos.

#### **3.3.1.4 Cuartos de Telecomunicaciones**

Cada uno de los bloques del edificio cuentan con un cuarto de telecomunicaciones lo cual facilita la administración y distribución del cableado de red.

Los rack de cada uno de los bloques son tipo gabinete, los mismos que se mantienen cerrados bajo llave y su administración se encuentra a cargo del personal de Redes, permitiendo de esta forma llevar un control sobre el personal que ingrese a los mismos.

Los racks poseen patch panel para voz y datos, sin embargo en algunos casos no se procede con el uso correcto. Ciertos puertos de voz se los está utilizando para datos y viceversa, afectando a la estética y administración de los mismos.

En ciertos racks como Bloque Recreacional, Servicios complementarios no existen organizadores verticales y los organizadores horizontales existentes no son utilizados correctamente, por lo cual se evidencia desorden en los patch cord instalados.

Dentro de los cuartos de telecomunicaciones pasan los ductos de la tubería de agua lo cual causa humedad a los mismos y puede provocar un acelerado deterioro del cableado.

Las luminarias de los cuartos de telecomunicaciones son lámparas fluorescentes y se encuentran ubicadas a distancias no apropiadas de los racks. Las luminarias emiten campos electromagnéticos y al estar situados a cortas distancias de los racks, causan interferencia en la transmisión de los datos.

En caso de fallas de energía no se cuenta con lámparas de emergencia dentro de los cuartos de telecomunicaciones.

Las bandejas horizontales y verticales soportan tanto el cableado de datos como el cableado eléctrico sin una debida organización de los mismos.

#### **3.3.1.5 Data Center**

Los rack del Data Center albergan el servidor de que se encuentra instalado improvisadamente y se encuentra sobre una caja fuera del rack.

Existe un sistema de aire acondicionado en el Data Center que permite que la temperatura se mantenga entre 20<sup>0</sup> y 23<sup>0</sup> C, constituyendo una temperatura óptima para su operación.

Todo el equipamiento activo y servidores de aplicaciones se encuentran conectados a la red estandarizada o tomas reguladas, protegiéndolos ante fallos de energía.

Todos los rack del complejo cuentan con una conexión hacia el sistema de puesta a tierra tipo malla que los protege ante corrientes de fuga y sobrecargas eléctricas.

Existe un UPS de 80 kVA que alimenta a los equipos de conmutación y servidores del Data Center en caso de fallas en la energía eléctrica. Adicionalmente se encuentran tres UPS ubicados en restaurante, recreacional y servicios complementarios de igual manera en cada uno de los bloques educativos.

El mantenimiento del Data Center es recomendable realizar periódicamente su limpieza; además se debe utilizar de mejor manera la ductería, techo falso, piso falso y bandejas existentes para la distribución del cableado de datos y eléctrico. Así también se recomienda utilizar los accesorios apropiados para el manejo del cableado los cuales protejan de tensiones y ángulos inapropiados en el recorrido del mismo.

Existen tres racks en el Data Center que cumplen diferentes funciones:

El primero es un rack de piso, en éste se encuentran los equipos de redes y telecomunicaciones como también 4 bandejas de fibra óptica (ODFs), UN Router Cisco 800 series para la conectividad con CNT. un switch HP 2910 2 24G , que da conectividad a los 4 enlaces

internos de fibra así como un Switch HP 1910 48G para la conectividad del Bloque Administrativo , un patch panel para la red de datos, un organizador horizontal de fibra óptica y dos organizadores horizontales para cable UTP; estos equipos permiten el funcionamiento de la red del complejo, al constituirse como el núcleo de la red interna.

El segundo rack es de piso, está destinado al todo lo referente a voz incluyendo patch panel para la red de voz y la central telefónica.

o El tercer rack es tipo de piso, este se encuentra sub utilizado ya que tiene un equipo de amplificación de audio para la periferia de igual manera en este se encuentra almacenado el panel de control de las cámaras IP.

A pesar de que el Data Center cuenta con sensores de humo para protección ante la presencia de fuego, este no es el único problema al cual se encuentra expuesto este lugar; es recomendable que se instale un sistema de monitoreo digital el cual pueda alertar al personal ante la presencia de valores anormales en la temperatura, humedad relativa, condensación del aire, entre otros, de manera automática. Así también es recomendable implementar un sistema de monitoreo en tiempo real que permita tener el control y registro de las labores realizadas en el interior del mismo.

### **3.3.1.6 Sistema de puesta a tierra**

El sistema de puesta a tierra del edificio protege tanto a los servidores como al equipamiento activo del mismo.

Se tiene una instalación de puesta a tierra tipo malla para protección de los equipos del Data Center, ante corrientes de fuga y sobrecargas eléctricas.

Cada uno de los rack del edificio cuentan con una conexión al sistema de puesta a tierra, sin embargo esta conexión no se encuentra debidamente etiquetada.

## **3.3.2 ELEMENTOS DE PARTE ACTIVA**

### **3.3.2.1 Equipos de red**

Los switches utilizados a nivel de usuario final en la red interna soportan la carga del complejo, así también al ser equipos administrables permiten configurar los mismos adecuándose a las necesidades que demande la red. Sin embargo estos equipos cuentan con una configuración básica.

El servicio de red inalámbrico es aplicado en el bloque administrativo, bloque educativo, Bloque recreacional, Restaurante, Servicios complementarios, y Residencia a través de equipos HP AP v M200.

Los switches de los bloques: Recreacional, Gimnasio de Potenciación, Restaurante, tienen un mínimo de puertos usados.

El switch correspondiente al bloque administrativo es el que tiene mayor carga de trabajo y el que genera mayor tráfico en lo que a puertos usados corresponde. Los switch de los tres bloques educativos igualmente tienen cableado una gran cantidad de puntos pero aún no se han usado cabe señalar además que por los problemas estructurales del bloque biblioteca el rack ha sido desinstalado para precautelar la integridad de los equipos.

No se cuenta con equipos de stand-by de reemplazo para un caso de malfuncionamiento de algún equipo activo.

El uso del CPU de los equipos de conmutación es relativamente bajo como se indica a continuación:

**Tabla 7. Uso de CPU de los switches**

ORD	MARCA	MODELO SERIE	UBICACIÓN	USO DEL CPU
1	Switch 3com	7700	ADMINISTRATIVO	12%
2	Switch 3com	5500	BLOQUE AULAS	0%
3	Switch CISCO	5500	BLOQUE LABORATORIOS	3%
4	Switch HP	1910 48G	BLOQUE BIBLIOTECA	0%
5	Switch CISCO	5500	SERVICIOS COMPLEMENTARIOS	11%
6	Switch CISCO	5500	RESTAURANTE	2%
7	Switch CISCO	5500	RECREACIONAL	2%

**Fuente: Javier Espinosa**

- Del análisis de la tabla 12 se deduce que los equipos trabajan con un bajo consumo de sus recursos, por ende la red todavía puede ser explotada con mayor cantidad de tráfico; en caso de que se sobrepase el 80% el uso del CPU de los equipos, se debería pensar en soluciones de equipos más robustos o realizar backups y balaceo de carga con otros equipos.

### **3.3.2.2 Equipos de Control y Seguridad**

La administración de los equipos de control de acceso por medio de huella dactilar (SOYAL AR.821 E/F), los cuales se encuentran uno en la segunda planta del edificio administrativo y otro en el bloque de servicios complementarios se la realiza desde el Cuarto de Control, por lo cual se ha utilizado un cable de red conectado directamente a un puerto del switch de bloque para su administración. Para un manejo adecuado del sistema de control ubicado en servicios complementarios es necesario ya crear una Vlan.

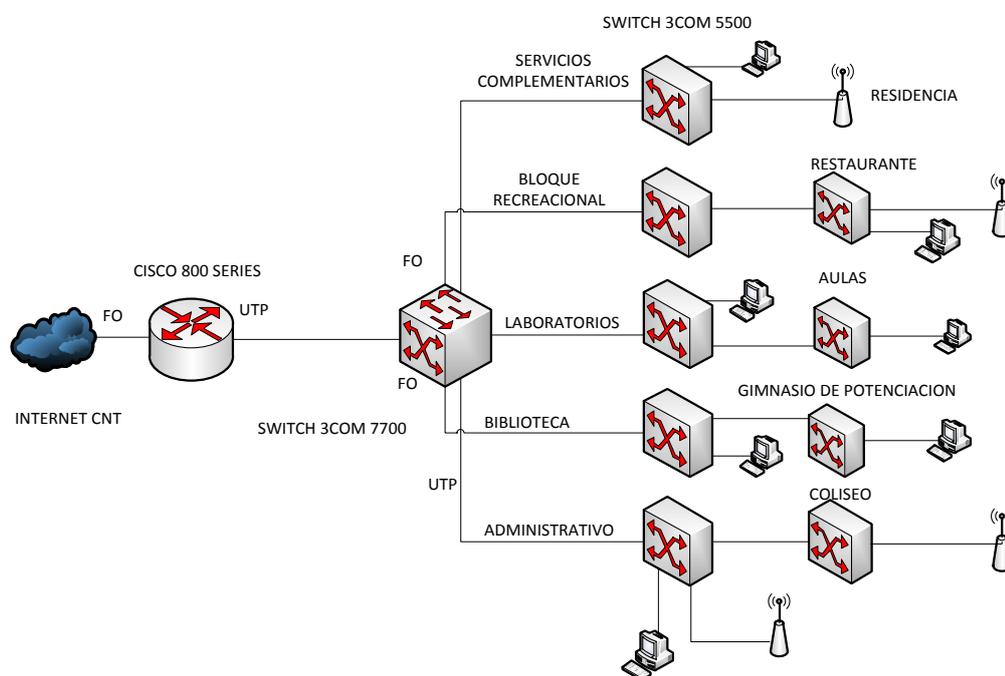
### **3.3.3 ESQUEMA DE LA TOPOLOGÍA DE RED ACTUAL**

Para el análisis de la topología de la red del complejo su estudio se divide en dos partes, una su topología externa desde la cual se provee el servicio para internet y otra la estructura interna a la cual se brinda los servicios de red.

### 3.3.3.1 Topología Física

La topología física de la red interna del Centro de Entrenamiento para el Alto Rendimiento Carpuela en estudio cuenta con una interface de entrada, para el servicio de Internet.

En la siguiente figura se muestra la estructura física de la red de la Institución.



**Figura 17. Topología física red interna**

**Fuente: Javier Espinosa**

Como se muestra en la figura anterior se pueden diferenciar dos redes: Red de Internet y LAN interna; las cuales están interconectadas por medio del switch CISCO 7700, como se detalla a continuación.

#### **Red de Internet**

El proveedor actual del servicio de Internet del CEAR es CNT, el cual tiene dos medios físicos para brindar el servicio; uno de ellos brindado

por medio del backbone de Fibra Óptica, y otro por medio de un radioenlace que se lo utiliza como backup.

El enlace de fibra óptica hacia la el complejo llega a un equipo conversor de fibra a Cobre para luego pasar hacia el switch CISCO 7700 al del edificio administrativo en el Data Center y desde allí se distribuye el servicio para los diferentes bloques del mismo.

Hacia las redes de Bloque educativo y Servicios complementarios de la Institución se manejan enlaces de fibra óptica.

### **Red LAN interna**

En el Data Center del edificio se encuentra instalado el switch CISCO 7700 del cual se deriva el backbone vertical del complejo, conformado por 4 enlaces de fibra óptica que llegan hasta los ODFs ubicados en: Bloque Laboratorio, Bloque Aulas, Bloque Biblioteca, Servicios Complementarios de Residencia en los cuales se tiene también switch CISCO 5500. De servicios complementarios de residencia se derivan conexiones a bloque recreacional y restaurante.

Al switch CISCO 7700 se encuentra conectado un PC administrador que realiza tareas administrativas como manejo de control de acceso, DHCP básicamente.

### 3.3.3.2 Topología Lógica

- La configuración actual no se ha considerado Vlans por lo tanto la red funciona como su topología física. Dejando las tareas administrativas a los switch para crear las redes por separado.
- Para el direccionamiento IP se utiliza subnetting, por lo cual no se tiene un direccionamiento eficiente provocando un desperdicio de las direcciones IP, a esto se suma la segmentación no adecuada y la falta de implementación de políticas en el tráfico interno.

Dentro de las configuraciones de los equipos de conmutación se puede destacar lo siguiente:

- Los equipos de conmutación se encuentran configurados con contraseñas de consola no seguras, además el acceso remoto se lo realiza vía Telnet, utilizando una conexión del tipo no segura.
- Los equipos de conmutación tienen configurado tres tipos de usuarios: monitor, manager y admin; las contraseñas de manager y monitor son las contraseñas establecidas por defecto por el fabricante.
- No se maneja políticas de control de seguridad a nivel de puertos, ni tampoco se controla el uso de las direcciones IP a nivel de usuario.

### **3.3.4 ANÁLISIS ESPECTRAL WIFI**

Para la observación del comportamiento del espectro radioeléctrico se realizaron pruebas de monitoreo utilizando un analizador de espectros de frecuencias Wi-Fi, donde se detectaron redes inalámbricas operando en los canales 1, 6 y 11 los mismos que trabajan a las siguientes frecuencias:

- Channel 1: 2412 MHz
- Channel 6: 2437 MHz
- Channel 11: 2462 MHz

De las pruebas realizadas se concluye que los canales se encuentran operando de manera óptica según las especificaciones de las normas IEEE 802.11b e IEEE 802.11g respetando la separación de los canales evitando que se produzcan interferencias entre los canales asignados, además se ha considerado valores reales desde los -70dBm a -120dBm.

### **3.4 INCUMPLIMIENTO DE NORMAS Y ESTÁNDARES DE CABLEADO ESTRUCTURADO**

Basados en las normas y estándares de cableado estructurado, durante el levantamiento de información se detectó el incumplimiento de algunas de ellas. Las más importantes se enumeran a continuación:

#### **3.4.1 CABLEADO HORIZONTAL**

- La norma ANSI/EIA/TIA 568 B establece:

- No deben existir empalmes a lo largo del cableado horizontal, sin embargo debido al mal dimensionamiento de los cables se ha colocado jacks flotantes y patch cords para reflejarse en el patch panel.
  
- Todas las conexiones realizadas hacia el área de trabajo deben ser correctamente protegidas, además las mismas no deben causar inconvenientes o problemas para los usuarios, pero algunas de las conexiones nuevas no tienen las debidas canalizaciones ni ductos necesarios como se detalló anteriormente.
  
- Se debe tener un máximo de llenura en los conduit instalados del 40%, sin embargo se permite hasta un máximo de llenura del 60% cuando se han debido realizar adiciones no planeadas luego de la instalación inicial, no obstante, los conduit instalados en el complejo no permiten adición en los mismos y algunos de los cables de red instalados no cuentan con ningún tipo de protección como es el caso del cableado de cámaras externas, por lo cual para las nuevas conexiones que se realicen y las que se deban modificar, es necesario tener en cuenta la aplicación de la norma.

- La norma 606A indica el uso de etiquetas que aseguren su clara identificación y lectura de los puntos de red y de todas las conexiones realizadas, sin embargo durante el levantamiento de información se encontraron 30 puntos de red sin la debida etiquetación, así también algunos de los puntos de red que si bien cuentan con una etiqueta, éstas no son las más adecuadas debido a que su lectura puede ser confundida o en muchos casos ilegible, al no haberse utilizado los materiales adecuados.

#### **3.4.2 CABLEADO VERTICAL**

- Norma ANSI/EIA/TIA 569.
- Se debe usar conduit para proteger la fibra óptica o cable UTP utilizado como cableado de backbone, sin embargo el cableado vertical del edificio no cuenta con protección física alguna.
- Es necesario contar con diversos puntos de entrada para proveer el servicio de telecomunicaciones, asegurando la no interrupción del servicio por falla en la ruta. Al momento no se cuenta con redundancia del backbone principal por lo cual de existir una falla del canal, la red quedaría parcial o totalmente fuera de servicio.

### 3.4.3 CUARTOS DE TELECOMUNICACIONES

- En los cuartos de telecomunicaciones las luminarias instaladas y los cables de energía eléctrica no cumplen la norma ANSI/EIA/TIA 569 en donde se especifica los requisitos mínimos para separación entre circuitos de alimentación (120/240V, 20 A) y cables de telecomunicaciones:
  - o Los cables de telecomunicaciones deben estar separados físicamente de los conductores de energía eléctrica;
  - o Si dichos conductores pasan por la misma canaleta o bandeja deben estar separados por barreras entre el cableado lógico y eléctrico;
  - o Dentro de las cajas de distribución o compartimentos de tomas, debe haber separación física total entre los cableados.
- Para reducir el acoplamiento de ruido producido por cables eléctricos, fuentes de frecuencia de radio, motores y generadores de energía eléctrica, se deben considerar las siguientes precauciones:
  - o Uso de protectores contra irrupción en las instalaciones eléctricas para limitar la propagación de descargas.
  - o Uso de canaletas o conductos metálicos, totalmente cerrados y puestos a tierra, o uso de cableado instalado próximo a superficies metálicas puestas a tierra.

- Los cuartos de telecomunicaciones deben estar libres de cualquier amenaza de inundación. No debe haber tubería de agua pasando por (sobre o alrededor) el cuarto de telecomunicaciones. De haber riesgo de ingreso de agua, se debe proporcionar drenaje de piso.
- Se debe emplazar instalaciones secas de supresión de fuego para contrarrestar los peligros de incendios en los mismos.
- Como retardante del fuego se recomienda cubrir un mínimo de una de las paredes con plywood de 19mm, de preferencia sin vacíos, con 2.4m de alto y bien fijado a la pared.
- Se deben instalar luces y señales de emergencia, emplazadas de manera que no se obstaculice la salida de emergencia. La señalización usada en los cuartos de telecomunicaciones debe ser desarrollada en base a un plan de seguridad del edificio.

#### **3.4.4 DATA CENTER**

- Se debe contar con diversos puntos de entrada para el servicio de telecomunicaciones, asegurando la no interrupción del mismo por falla en la ruta del enlace, permitiendo la continuidad de servicio y las necesidades existentes. Adicionalmente se deben escoger vías alternas para su instalación.
- Dentro del Data Center se deben considerar medidas de supresión de fuego secas, previniendo de esta manera riesgo de incendios y daños en el equipamiento.

- Se debe tener en cuenta medidas contra la filtración de agua, además, de existir riesgo de inundación se recomienda instalar desagües de piso, adicionalmente es necesario la instalación de un sistema de monitoreo constante para detectar cualquier anomalía.
- El Data Center debe tener un control y mantenimiento adecuado. Los pisos, paredes y techo deben ser tratados con productos especiales para eliminar el polvo, así también el suelo debe tener propiedades antiestáticas.
- Se recomienda que un mínimo de una de las paredes del Data Center deben estar cubiertas con plywood de 19mm, de preferencia sin vacíos, a una altura de 2.4m y bien fijado a la pared, su uso actúa como un retardante ante la presencia de fuego.
- Las puertas deben ser de mínimo 0.9 metros de ancho y dos metros de altura, y con facilidad de remoción.
- Es necesario realizar un estudio de la carga permitida por el piso, de manera que la concentración de equipos no exceda el límite de carga por metro cuadrado.
- Se debe contar con una operación continua del sistema de aire acondicionado o sistema de enfriamiento. La temperatura y humedad debe ser controlada proveyendo una continua operación entre los rangos de 18°C a 24°C con 30% a 55% de humedad relativa. Estas medidas deben ser realizadas a 1,5 m del suelo.

- Se deber instalar luces y señales de emergencia, las cuales deben ser emplazadas sin obstaculizar la salida de emergencia. La señalización usada
- en los cuartos de telecomunicaciones debe ser desarrollada en base a un plan de seguridad del edificio.

### **3.5 PARÁMETROS DE RENDIMIENTO DE LA RED ACTUAL**

Dentro del levantamiento de información es importante tener en cuenta los parámetros para medir el rendimiento de la red actual como los que se detalla a continuación:

#### **3.5.1 FLEXIBILIDAD**

La red del CEAR Carpuela maneja una estructura de topología en estrella, mediante la cual se facilita la adición, modificación o eliminación de puntos de red. Aunque su topología de red soporta nuevos cambios el equipamiento en muchos casos no lo soporta.

#### **3.5.2 DISPONIBILIDAD**

Aunque actualmente en la red no existen mecanismos para determinar la disponibilidad de la misma, esta no puede brindar una disponibilidad total a nivel de red debido a que:

- A nivel de la red interna no se cuenta con enlaces redundantes hacia los principales equipos de conmutación por lo cual de producirse daños o problemas en su conexión la red quedaría parcial o totalmente fuera de servicio.

Sin embargo es necesario considerar que en caso de fallas de los canales físicos o de los equipos de conmutación internos la red quedaría fuera de servicio, caso contrario es importante considerar lo siguiente:

- La capacidad de procesamiento de los servidores utilizados es mínima para el manejo de tráfico generado, por lo cual no se presenta interrupción en el servicio prestado hacia la red de datos.
- El backbone vertical se lo realiza a través de fibra óptica y cable par trenzado Cat 5e, los mismos que soportan el tráfico que fluye por la misma.
- En caso de fallas del suministro de energía local se cuenta con UPS que evitan los cortes de energía en la red, por tanto se asegura su operatividad.

### **3.5.3 ESCALABILIDAD**

El equipamiento del CEAR Carpuela, presenta factibilidad de crecimiento de usuarios en la red. Es importante considerar que el equipamiento que se maneja posee características escalables ya que permite apilar hasta ocho switches de las mismas características, con lo cual se solucionaría un posible inconveniente de disponibilidad de puntos de red.

### **3.5.4 RENDIMIENTO**

Todo el equipamiento de red del Complejo es administrable, además su capacidad de procesamiento permite manejar grandes cantidades de tráfico como se determinó anteriormente, así también el uso de CPU se encuentra en niveles muy bajos lo cual indica que se puede manejar niveles más altos de tráfico sin ningún tipo de inconveniente. Es importante considerar que el equipamiento que se maneja a nivel interno es de gama alta, el cual como se determinó soporta nuevas aplicaciones de red.

### **3.5.5 DOMINIOS DE BROADCAST**

Los dominios de Broadcast del complejo se los encuentra definidos en base a bloques, más no en base a un estudio por dependencias o funciones, el cual no es óptimo.

### **3.5.6 SEGURIDAD**

- No existen políticas definidas a nivel de puertos del equipamiento activo para limitar el uso de los mismos a una sola dirección MAC e IP, por lo cual al momento, más de un equipo de cómputo puede utilizar un mismo punto de red sin que se tenga un control de esto. Las personas que conocen el procedimiento para cambiar la configuración de una tarjeta de red, podrían configurar a otro equipo o incluso al mismo con una dirección diferente a la asignada lo cual desemboca en un uso indiscriminado del direccionamiento IP; al no existir políticas bien definidas sobre el uso de la red, no se puede establecer sanciones cuando se incurra en el incumplimiento de normas del uso de la red.
- El acceso hacia los equipos de conmutación no se encuentra debidamente configurado ya que al contar con diferentes niveles de acceso como se explicó anteriormente y al permitirse el acceso por medio de sesiones no seguras, alguna persona con intenciones maliciosas podría ingresar a los mismos y realizar cambios o modificaciones de las configuraciones ocasionando la denegación del servicio, entre uno de sus inconvenientes.

## **4 CAPITULO IV. DISEÑO DE TOPOLOGÍAS FÍSICA Y LÓGICA PARA LA RED DE DATOS**

### **4.1 INTRODUCCIÓN**

El desarrollo del presente capítulo muestra el diseño para la red de datos de la institución, el cual enumerará aspectos relevantes a tomarse en cuenta para su implementación. Antes de realizar el rediseño de la red de datos, es importante considerar aspectos fundamentales para el mismo como son la proyección del crecimiento de la red, las políticas de red manejadas en su interior y los requerimientos de los usuarios de la infraestructura.

### **4.2 ESTUDIO DE LA PROYECCIÓN DE CRECIMIENTO DE RED EN LA INSTITUCIÓN (Ministerio Del Deporte Ecuador, 2014)**

Para el estudio de la proyección de crecimiento de red en el CEAR Carpuela se ha tomado como base la información brindada por el Departamento de Sistemas, en función de la cual se determinó que su crecimiento no se basa en el aumento del personal, debido a que la institución no tiene incrementos del mismo con el paso de los años (para determinar la necesidad de contratación de nuevo personal es necesario modificar su estructura orgánica), ya que el número de plazas de trabajo es fijo.

Sin embargo, la masificación del uso de las TIC ha demandado la instalación de más puntos de red, previendo alcanzar un número máximo igual al número del personal contratado.

Se estima que para el siguiente año se cuente con 63 puntos de red de datos, teniendo de esta manera una infraestructura completamente operativa; para esto es necesario considerar que un crecimiento en la infraestructura de cableado estructurado lleva consigo la demanda de equipamiento de red.

### **4.3 POLÍTICAS EN LA RED**

Actualmente la red del CEAR no cuenta con políticas definidas sobre el uso de la misma, sino más bien esta se rige en base a un conjunto de necesidades mínimas operativas. Dentro de las normas de red implementadas se tiene:

#### **4.3.1 CUARTOS DE TELECOMUNICACIONES**

- El acceso hacia los cuartos de telecomunicaciones que en este caso particular del Complejo nos referimos a Racks de piso de cada Bloque se encuentra restringido al personal de Administradores de Red, quienes son los encargados de manejar las llaves de las puertas de ingreso a los mismos. Si el personal de administración de la red telefónica necesita ingresar a los cuartos de telecomunicaciones, éstos deben solicitar su ingreso al personal de administración de red del CEAR.

### **4.3.2 DATACENTER**

- El acceso hacia el Data Center está limitado al personal de administración de la red; así también la administración de los diferentes sistemas de aplicación de la Institución están restringidos al personal de Informática del área.
- Sólo personal autorizado puede ingresar hacia el Data Center, quienes deberán portar las respectivas tarjetas de ingreso.
- Todo acceso hacia el Data Center debe ser registrado en el libro destinado para ello, indicando los nombres de las personas que ingresen, la hora tanto de entrada como de salida y el trabajo realizado en el mismo.

### **4.3.3 EQUIPAMIENTO ACTIVO Y SERVIDORES**

- Las contraseñas de administración del equipamiento activo deben ser manejadas de forma exclusiva por los administradores de red de la institución.
- Las contraseñas de los servidores de aplicaciones deben ser manejadas de forma exclusiva por el personal de administración de los sistemas, con conocimiento del supervisor de la sección.

#### **4.3.4 RED INALÁMBRICA**

- La red inalámbrica del edificio es utilizada como servicio agregado a los usuarios del CEAR siendo este de acceso total al internet sin ninguna contraseña.

#### **4.3.5 EQUIPOS DE CÓMPUTO**

- Todos los equipos de cómputo de la Institución deberán formar parte del directorio activo.
- Cada usuario contará con su respectiva cuenta de usuario y contraseña para el ingreso hacia los equipos computacionales.

### **4.4 ANÁLISIS DE REQUERIMIENTOS DE USUARIOS**

Antes de realizar el diseño de la red de datos de la Institución es necesario determinar los requerimientos para la red por parte de los usuarios de la misma, de manera que el diseño realizado sea funcional. Dentro de los requerimientos de red reportados por los usuarios durante el levantamiento de información se tienen:

#### **Adición de puntos de red.**

Teniendo en cuenta la masificación de las TIC`s, es necesario estudiar los requerimientos de cada uno de los departamentos para determinar de esta manera la necesidad de adición o modificación de puntos de red. Por varios de los motivos indicados en el capítulo anterior se precisa la implementación de nuevos puntos de red, su resumen en base a los bloques del edificio se muestra en la siguiente tabla:

**Tabla 10. Resumen de requerimientos de red de la institución**

BLOQUE	REQUERIMIENTO
ADMINISTRATIVO	8
MEDICO	5
AULAS	12
LABORATORIOS	12
BIBLIOTECA	6
RECREACIONAL	10
SERVICIOS COMPLEMENTARIOS	6
RESTAURANTE	4

**Fuente: Javier Espinosa**

### **Acceso a la red inalámbrica.**

Es preciso considerar la necesidad de habilitar una limitación al acceso servicio de red inalámbrica para limitar el uso indiscriminado de ancho de banda.

### **Acceso a las aplicaciones.**

Cada uno de los nuevos puntos de red que se instalen en el edificio deben tener acceso hacia todas las aplicaciones internas. El detalle de los servidores y aplicaciones contenidas se muestran a continuación:

- Servicio de antivirus.
- Correo electrónico institucional.
- Acceso a los portales web institucionales internos.
- Acceso a un portal web de intranet.
- Sistema documental.
- Sistema de inventarios.
- Directorio Activo.

- Acceso a Internet (en función de la necesidad, autorizada por el ente rector).
- Servicio de impresión.
- Servicio de compartición de archivos.
- Servicio de resolución de nombres interno.

Así también el acceso hacia las aplicaciones de la red interna como externa deben ser fiables y confiables, mejorando su velocidad de acceso y asegurando su disponibilidad.

#### ***4.5 REINGENIERÍA DE LA RED DE DATOS DEL CENTRO DE ENTRENAMIENTO PARA EL ALTO RENDIMIENTO DE CARPUELA.***

Luego de realizado el análisis de la información referente al estudio situacional de la red de la institución en el capítulo anterior y conociendo su estructura interna, a continuación se plantea el rediseño de la red de datos del complejo, partiendo de su estructura lógica y física estudiada, la cual provea una red escalable, flexible, fácilmente administrable, además disponible, la misma que reduzca el tamaño de los dominios de broadcast existentes permitiendo una solución integral para la red de datos de la institución. Así también el diseño propuesto mejorará el rendimiento de la red al aprovechar óptimamente el equipamiento existente con una administración adecuada, efectuando cambios drásticos sobre la misma. La reingeniería de red parte del análisis de diseño a nivel de cableado estructurado y a nivel de la parte activa como se aprecia más adelante.

## **4.5.1 CONSIDERACIONES DE DISEÑO**

### **4.5.1.1 Cableado Estructurado**

Es importante tener en cuenta aspectos relacionados al cableado estructurado ya que el funcionamiento lógico de la red depende de su parte física. A continuación se recogen algunas de las consideraciones para el diseño del cableado estructurado.

#### ***4.5.1.1.1 Cableado Horizontal***

- La necesidad de adición de puntos de red en varios departamentos de la institución debe ser validada en base al levantamiento de información realizado, con lo cual se brinde el servicio de red requerido por los usuarios.
- Para la ampliación del cableado horizontal se debe tener en cuenta el crecimiento estimado de la red, de manera que se brinde un servicio de red completo a todos los usuarios, tanto en la actualidad como en el futuro.
- Las nuevas conexiones de red no deben sobrepasar las distancias permitidas por la norma, además éstas deben seguir las rutas predefinidas y cumplir las demás especificaciones de las normas de cableado estructurado.
- Se debe realizar una reorganización de cables de red y cables eléctricos en las bandejas de distribución, separándolos físicamente los unos de los otros para evitar la interferencia electromagnética entre ellos.

- Todas las conexiones realizadas deben estar debidamente documentadas y etiquetadas de manera que permitan una clara identificación de las mismas. Así también se debe tener en cuenta que la etiquetación realizada en la institución debe permitir una fácil identificación respecto al servicio prestado y su ubicación; mediante el levantamiento de red realizado se ha determinado que el etiquetado utilizado no es el más adecuado, por lo cual se sugiere que se realice una nueva identificación y etiquetación de los puntos de red, además debe tenerse en cuenta que todos los puntos que se han añadido cuentan con una etiquetación no adecuada o simplemente no la tienen.

### **Propuesta de una nueva etiquetación**

Los parámetros a tomarse en cuenta para la realización de una nueva identificación de los puntos de red en la institución son:

- **Bloque:**

Permite una fácil identificación del bloque al cual se brinde el servicio de red.

**Tabla 11. Nomenclatura utilizada para los bloques**

<b>BLOQUE</b>	<b>NOMENCLATURA</b>
BLOQUE ADMINISTRATIVO	B1
AULAS	B2
LABORATORIOS	B3
BIBLIOTECA	B4
SERVICIOS COMPLEMENTARIOS	B5
RESTAURANTE	B6
BLOQUE RECREACIONAL	B7

**Fuente: Javier Espinosa**

- **Tipo de servicio (Tipo):**

Permite determinar el tipo de servicio prestado sea de voz o de datos.

**Tabla 12. Nomenclatura utilizada para el tipo de servicio**

VOZ	V
DATOS	D

**Fuente: Javier Espinosa**

**Número de Patch Panel (#PP):**

Permite identificar el patch panel en el cual se encuentra conectado el punto de red.

**Tabla 13. Nomenclatura utilizada para el número de PP**

PP UNO	1
PP DOS	2
PP TRES	3

**Fuente: Javier Espinosa**

- **Número del Punto de Red:**

Permite identificar el número del punto de red según su ubicación en patch panel con su correspondiente salida a nivel de punto de red en las salidas de telecomunicaciones. Su identificación se la realizará utilizando los número del 01 al 48, para facilitar su lectura.

**Ejemplo:** El punto de red de datos D-025 ubicado en el patch panel 1 del Bloque 1 se lo etiquetaría como:

**B1D1-25**

Bloque *Tipo* # PP # Punto de Red

**Ejemplo de propuesta de etiquetación**

Esta nueva etiquetación permitirá tener una idea clara de la ubicación del punto de red en cuestión, identificando claramente el bloque, el servicio prestado y su ubicación en patch panel.

#### **4.5.1.1.2 Cableado Vertical**

Del estudio realizado se ha verificado que dos de los bloques del edificio cuentan con backbone principal de cable UTP; considerando que por este canal se maneja una cantidad moderada a mínima de tráfico perteneciente a los usuarios de cada uno de los bloques, es importante asegurar que no existan cuellos de botella en la red, por lo cual es recomendable en un futuro analizando el crecimiento que se remplace estos enlaces de cable UTP por enlaces de fibra óptica, teniendo en cuenta que el equipamiento existente entre ellos lo soporta, de manera que se asegure conexiones a Gigabit.

Para asegurar la disponibilidad de la red es necesario que se instale cableado de backup para lo cual se podría considerar dos opciones, una en la cual se utilice otros enlaces de fibra óptica, o la utilización de cableado par trenzado UTP Cat 6a. De instalarse enlaces de fibra óptica se aseguraría dos rutas que brinden conexiones a Gigabit Ethernet, sin embargo el instalar enlaces de cable UTP constituye una solución más económica y factible considerando que estos enlaces se los utilizaría netamente como backup.

Así también como se recomendó en el capítulo anterior es necesario que la fibra óptica cuente con protección, de manera que se evite que se produzcan fallos en la misma debido a la mala manipulación, además se debe tener en cuenta las normas de cableado estructurado para tender las mismas junto con su respectiva etiquetación.

#### **4.5.1.1.3 Cuarto de Telecomunicaciones**

Es importante considerar que para una mejor administración de la red, ésta debe contar con una debida organización por lo cual es necesario que todos los puntos de red lleguen hacia su respectivo patch panel para su distribución.

Se debe eliminar los puntos de red que se encuentran utilizando jack como extensión hasta llegar a patch panel, ya que esto además de que no está permitido por las normas de cableado estructurado también disminuye el rendimiento de la misma y aumenta los puntos de falla.

Es importante que todos los puntos de red instalados cumplan con las normas de cableado estructurado respetando la distancia hacia las tomas eléctricas, también es necesario que se separe el cableado de datos del cableado eléctrico, para evitar problemas de interferencia electromagnética. De igual forma las luminarias instaladas en los cuartos de telecomunicaciones deben mantener una adecuada separación de los rack de comunicaciones debido a la emisión de campo electromagnético que estas producen.

A lo largo de la distribución del cableado estructurado se recomienda que se utilicen los debidos accesorios para su correcta instalación, evitando ángulos y tensiones inadecuadas en los enlaces de conexión.

#### **4.5.1.1.4 Data Center**

Es necesario que se tenga un especial cuidado con el cumplimiento de las normas de cableado estructurado en este cuarto, ya que el mismo constituye un punto crítico en la red, tomando en cuenta algunos criterios básicos como:

- Es importante que se cuente con red eléctrica de respaldo de manera que no se tenga cortes de servicio por falla del suministro eléctrico.
- Se debe mantener un control sobre los elementos que constituyen el cableado de datos contando con los respectivos manejadores de cable y accesorios; así también es importante el uso adecuado de los patch panel que permitan una correcta administración de este cuarto.
- De igual forma para asegurar la conexión es preciso utilizar patch cords y cables de fibra óptica certificados lo cuales garanticen la conexión hacia el equipamiento activo y la zona de servidores.
- Se debe tener en cuenta realizar mantenimientos periódicos al sistema de aire acondicionado de manera que se mantenga una temperatura adecuada en el Data Center.

#### **4.5.2 POLÍTICAS DE ADMINISTRACIÓN DE LA PARTE ACTIVA**

Dentro de las políticas de seguridad para la parte activa se debe tener en cuenta lo siguiente:

- El acceso remoto debe ser encriptado utilizando protocolo SSH versión 2 de preferencia, los accesos vía telnet deben ser suspendidos definitivamente y se deben definir los equipos en la red que están autorizados a acceder a la administración de los mismos.
- Las interfaces de administración web deben ser deshabilitadas de forma definitiva o debe controlarse el acceso a las mismas únicamente desde los equipos de los administradores de red.
- Los administradores de red deben cambiar periódicamente las contraseñas de los equipos de parte activa, utilizando contraseñas seguras y encriptadas.

En los documentos de configuración debe explicarse detalladamente los comandos aplicados y su funcionalidad.

- La actualización de los IOS debe realizarse de forma periódica y debe tomarse en cuenta como un parámetro a definir periódicamente en el mantenimiento de los mismos.
- Se deben crear procesos y procedimientos que describan las acciones y eventos que se deban realizar en caso de que no se encuentre el personal de administración de la red. Además si se presentan nuevos eventos es necesario actualizar siempre estos procedimientos.

- Es importante tener una bitácora en la cual se registren todos los eventos suscitados en la red.
- Es necesario hacer el levantamiento de información relacionada a componentes de hardware y software de los equipos y dispositivos conectados a la red de datos de la Institución de manera que se pueda controlar el cambio y uso de los recursos existentes.
- Se debe aplicar una reingeniería según estándares internacionales para el mejoramiento del performance de dicha red, mediante la redistribución del equipamiento, creación de backups a todo nivel, incluidas las redundancias físicas; además se deben aplicar protocolos como Spanning Tree según los requerimientos para evitar que se produzcan lazos en la red.
- Se debe reestructurar la segmentación del tráfico para el mejor rendimiento de los departamentos que pertenecen a la red de la institución.
- Se recomienda implementar software libre de monitoreo y gestión que permita ver las características en tiempo real de la red, así como la disponibilidad del servicio de red.

#### **4.5.3 MODELO DE RED**

La solución de rediseño para la red de datos del complejo debe permitir que la red sea fácilmente administrable, con facilidad de expansión, disponible, segura y con la capacidad de resolver los problemas con rapidez; estas características son brindadas por un modelo de red del tipo jerárquico.

El modelo de diseño jerárquico típico se separa en tres capas:

**Capa de acceso:** Es la interfaz con los dispositivos finales. Esta capa de acceso puede incluir routers, switches, puentes, hubs y puntos de acceso inalámbricos. Los switches de la capa de acceso facilitan la conexión de los dispositivos de nodo final a la red. Por esta razón, necesitan admitir características como seguridad de puerto (el switch decide cuántos y qué dispositivos se permiten conectar), VLAN, Fast Ethernet/Gigabit Ethernet, PoE, QOS y agregado de enlaces.

**Capa de distribución:** La capa de distribución controla el flujo de tráfico de la red con el uso de políticas y traza los dominios de broadcast al realizar el enrutamiento de las funciones entre las VLANs definidas en la capa de acceso. Presentan disponibilidad y redundancia altas para asegurar la fiabilidad. Los switches de capa de distribución recopilan los datos de todos los switches de capa de acceso y los envían a los switches de capa núcleo. Los switches de capa de distribución proporcionan funciones de enrutamiento entre las VLAN (y por lo tanto funciones de la Capa 3), utilizan listas de control de acceso (ACL), agregado de los enlaces (tanto a la capa de acceso como a la capa de núcleo), tienen más de una fuente de alimentación, deben respetar la QOS aplicadas en los switch es de acceso y deben tener una tasa de envío alta. Los switches más nuevos de capa de distribución admiten enlaces de 10Gb.

**Capa núcleo:** Interconecta los dispositivos de la capa de distribución y puede conectarse a los recursos de Internet. El núcleo debe estar disponible y ser redundante. Los switches de capa núcleo requiere manejar tasas muy altas de reenvío, agregación de enlaces (de 10Gb con los switch de agregación), soporte de capa 3, suelen tener redundancia a nivel 3 (más rápida en converger que a nivel 2), enlaces Gigabit Ethernet/10 Gigabit Ethernet, componentes redundados (como la fuente de alimentación), suelen contar con opciones de refrigeración más sofisticadas (alcanzan mayor temperatura por la carga de trabajo), con hardware que permite el cambio en caliente y QOS.

#### **MODELO DE NUCLEO COLAPSADO. (CCNA, 2011)**

Un modelo de núcleo colapsado es aquel que combina la capa de distribución y la capa núcleo.

#### **JUSTIFICACION DE DISEÑO DE RED DE NUCLEO COLAPSADO.**

Como podemos observar en base a las necesidades de la red y al numero de usuarios de la misma es relativamente pequeña y en base al estudio de crecimiento podemos optar por este modelo de red.

Al eliminar una de las capas, eliminamos los equipos que están en ella, y por tanto es menos dinero a invertir.

Los equipos de hoy en día traen consigo muchas funcionalidades (Protocolos, configuraciones, medidas de seguridad, etc.) y capacidades

(velocidad de conmutación, densidad de puertos, etc.) comunes a ambas capas y por tanto no hacen necesario segmentarlo de esta manera.

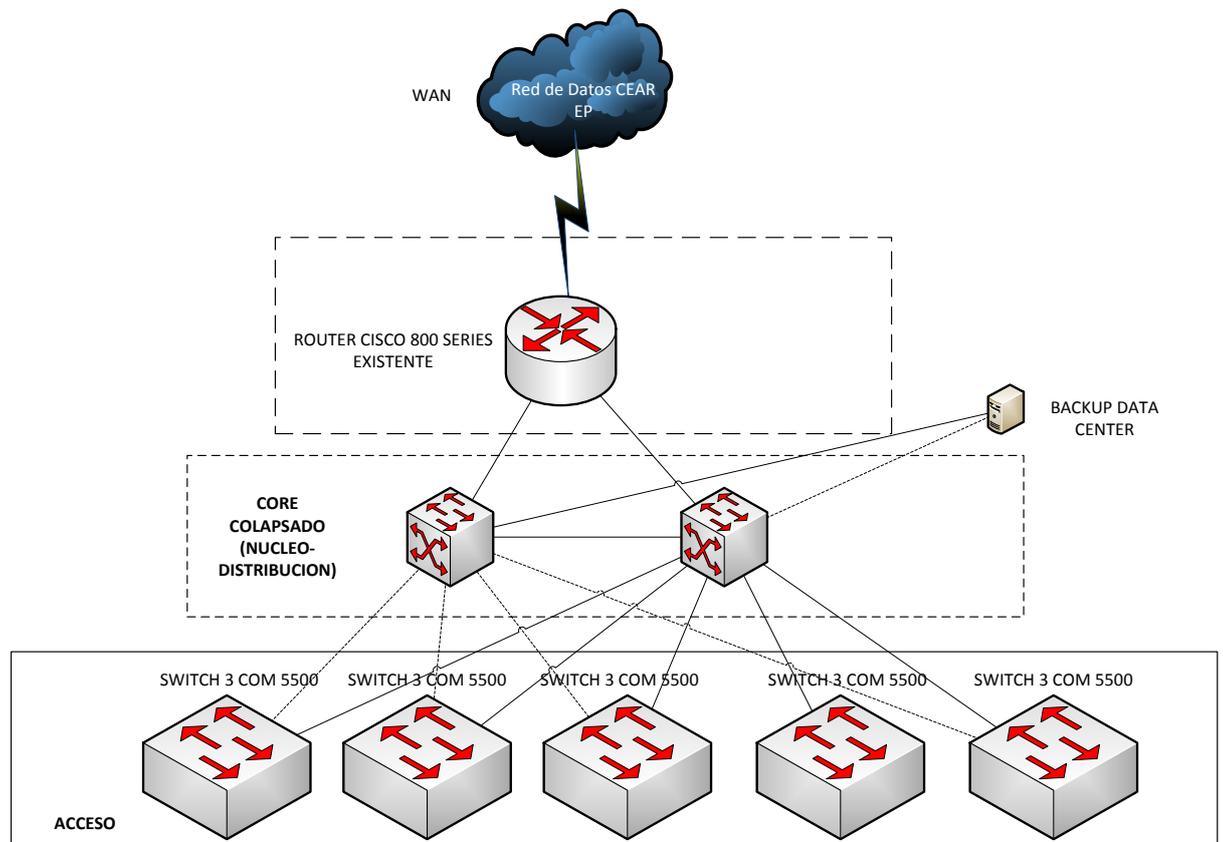
### **Beneficios de una red jerárquica:**

- **Escalabilidad:** Pueden expandirse con facilidad.
- **Redundancia:** Los switch se suelen conectar a varios switches de la capa superior.
- **Rendimiento:** El alto rendimiento de los switches de distribución y núcleo hacen que la información vaya a casi la velocidad del cable.
- **Seguridad:** Es posible configurar los switches de la capa de acceso con varias opciones de seguridad del puerto que proveen control sobre qué dispositivos se permite conectar a la red. Además, se cuenta con la flexibilidad de utilizar políticas de seguridad más avanzadas en la capa de distribución.
- **Facilidad de administración:** Los switches de una misma capa tienen una configuración similar.
- **Capacidad de mantenimiento.**

Principios para el diseño de una red:

- **Diámetro de la red:** Es el número de dispositivos que un paquete debe atravesar antes de alcanzar su destino. Mantener bajo el diámetro de la red asegura una latencia baja y predecible.

- **Agregado de ancho de banda:** En una red jerárquica si se ven necesidades de ancho de banda se puede crear un EtherChannel (agregado de enlaces) y aumentarlo.
- **Redundancia:** Se puede proveer redundancia duplicando las conexiones de red entre los dispositivos o duplicando los propios dispositivos.
- **Se comienza por la capa de acceso:** Una vez analizado el número de dispositivos y los requerimientos de estos se elegirán cuales y cuantos equipos de acceso se pondrán. En base al número de equipos de acceso se determina cuantos switchs de capa de distribución son necesarios y en base a estos los de capa del núcleo.



**Figura 18. Modelo de red Propuesto**  
**Fuente: Javier Espinosa**

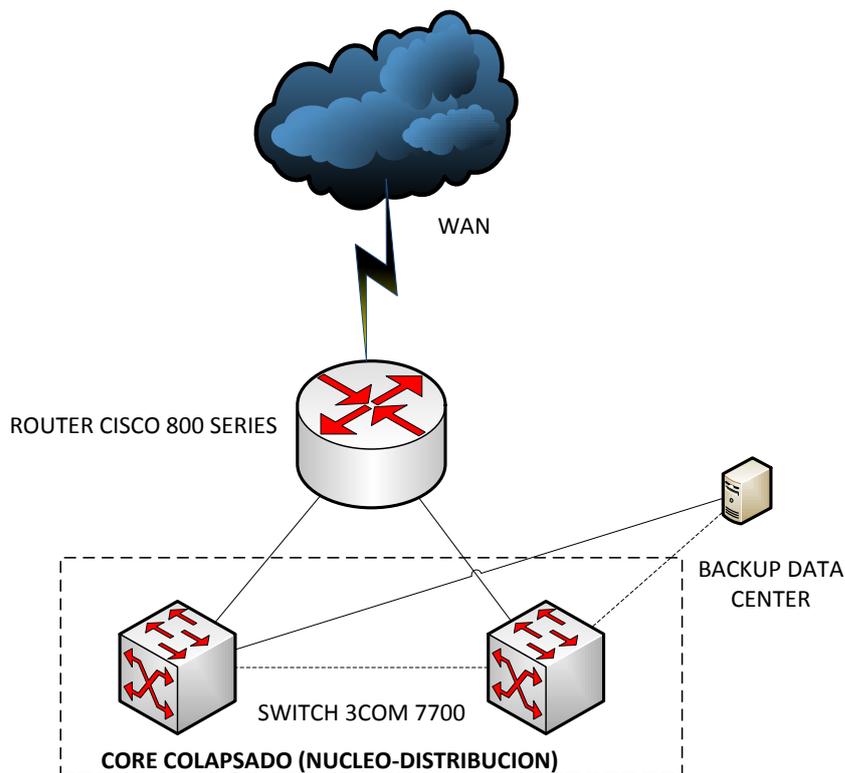
En la figura se observa de forma general el modelo de red planteado para la institución, en base al cual para cada una de las capas se definirá su funcionalidad, equipamiento y características propias de cada una de ellas. Dentro de las ventajas del modelo se destacan las siguientes:

- **Escalabilidad:** fácil crecimiento y expansión, su crecimiento se realiza desde el nivel de acceso hacia el nivel de núcleo, según la necesidad y la disponibilidad de puertos.

- **Rendimiento:** los switches de núcleo y distribución al tener buenas características manejan grandes velocidades, evitando tener cuellos de botella en la red.
- **Seguridad:** se permite manejar políticas tanto en los switches del nivel de distribución como en los switches del nivel de acceso permitiendo establecer políticas hasta a nivel de puerto.
- **Redundancia:** permite tener alta disponibilidad en la red, evitando tener caídas de servicio en la misma.
- **Aislamiento de fallas:** permite aislar equipos defectuosos de manera que no se vea afectado todo el rendimiento de la red, limitando el daño al segmento respectivo.
- **Administración y gestión de red:** brinda facilidad de administración al manejar una estructura por capas, además de una fácil gestión de la red.
- En el diseño se han considerado tres parámetros: ancho de banda, redundancias y diámetro de la red. Se considera que debe existir un ancho de banda de mayor a menor desde el nivel de núcleo hasta el nivel de acceso. Las redundancias que se proponen brindan disponibilidad a la red, por lo cual se deben duplicar las conexiones y el equipamiento. Se ha considerado las medidas del diámetro de la red en función de la mayor cantidad de equipamiento, la misma que es de tres.

#### 4.5.3.1 Nivel de núcleo-Distribución.

Como podemos ver, se colapsan las dos capas de “Core” y “Distribución”. Es un entorno que ofrece redundancia entre los equipos de acceso situados en la parte inferior de la imagen y los servidores en la superior. Tras haber evaluado las características de los equipos, éstos soportan protocolos de alta disponibilidad como HSRP, VRRP, STP, etc; también disponemos de enlaces redundantes tanto desde los switches de acceso, sw-of-01, así como como entre switches de Core/Distribución que nos proporciona una tolerancia ante fallos. Contando de que éstos tengan puertos a 1 Gbps podremos agregar enlaces(Etherchannel) para vencer posibles cuellos de botella al conectar más switches de acceso; también podremos implementar “Listas de Control de Acceso” (ACLs); y como no, al ser equipos de L3 configurar algún protocolo de enrutamiento (OSPF, EIGRP) o enrutado manual para el envío de paquetes.



**Figura 18. Nivel de distribución del modelo de red**  
**Fuente: Javier Espinosa**

En la capa de distribución es importante que se maneje un tipo de equipamiento con buenas características de rendimiento además de que el mismo brinde disponibilidad y fiabilidad.

La institución cuenta con equipamiento marca 3Com de la serie 7700 el cual es un switch capa 3 modular, éste se adapta de forma apropiada al modelo de red planteado, dado que entre sus principales características tiene soporte de L2 y L3, soporte de switching 10Gigabit, Gigabit y Fast Ethernet, soporte de PoE, soporte de ACL, MSTP, SNMPv3, soporte de agregados de enlace y manejo de una plataforma de chasis, permitiendo agregar nuevos módulos de requerir crecimiento a nivel de puntos de red.

#### **4.5.3.1.1 Consideraciones de diseño**

- El 3Com de la serie 7700 del cuarto de control manejará los enlaces de conexión con los bloques del complejo, además los enlaces de conexión hacia los servidores de aplicación; así también el switch manejará todo el tráfico generado en la red interna y tendrá a cargo el manejo de inter VLANs de la red.
- Debido a que éste equipo será el backbone de la red interna es recomendable usar un switch adicional de backup para asegurar el rendimiento de la red y evitar caídas de servicio en la red interna de la institución; es importante contar con redundancia tanto a nivel del equipamiento activo como a nivel del backbone asegurando la conexión con los equipos de la capa de acceso como con la capa de núcleo, para la cual como se mencionó anteriormente es posible realizar los enlaces de backup con fibra óptica o con cableado UTP según las necesidades y recursos de la Institución.

#### **4.5.3.1.2 Requerimientos:**

- En base al estudio realizado en el capítulo anterior y teniendo en cuenta el crecimiento de la red no se requiere la adquisición de otro equipo ya que hay disponibilidad de puertos.
- Adicionalmente para contar con disponibilidad en la red es necesario contar con el equipamiento para backup el cual debe poseer

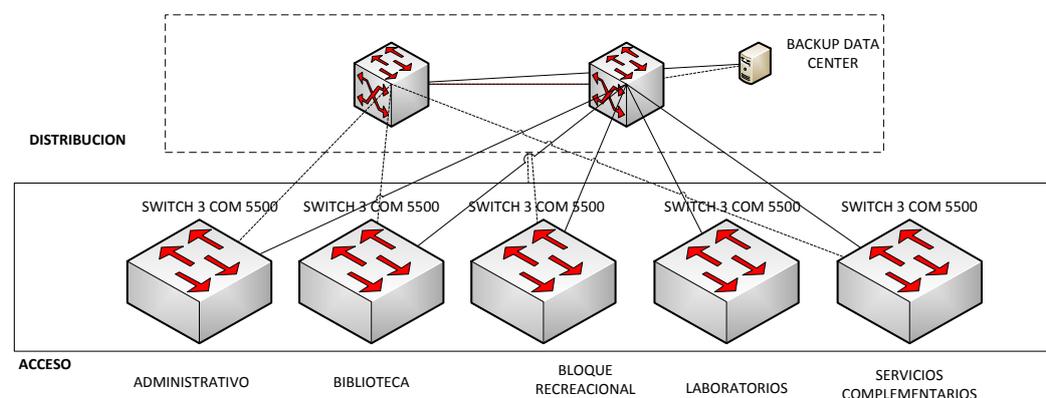
características similares al equipo de distribución principal de manera que este equipo ofrezca las mismas funcionalidades de red como las que se menciona a continuación:

- **Soporte de Capa 3.**
- **Políticas de seguridad y ACL:** soporte de seguridad a nivel de puerto y manejo de listas de acceso para permitir o negar el tráfico generado en la red.
- **QoS:** en caso de que se pretenda usar telefonía IP o IPTv en futuras aplicaciones y se tenga que priorizar el envío del tráfico por la red.
- **Alta tasa de envío:** con un alto backplane soportando aplicaciones de red exigentes (disponibilidad del 99,999%) y cumpliendo con los requerimientos.
- **Gigabit Ethernet y 10 Gigabit Ethernet:** para futuras aplicaciones y conforme el crecimiento de la red se recomienda realizar un upgrade a los equipos y aumentar módulos de 10 Gigabit Ethernet.
  
- **Componentes redundantes:** por lo que ya se ha mencionado y justificado anteriormente es necesario tener una redundancia de equipos y de conexiones.
  
- **Agregado de enlaces:** por medio de este método es posible aumentar el rendimiento del equipamiento activo.
  
- **Velocidad de cable:** definida por la capa física de red.

- Para el backup a nivel de conexiones de red es necesario el tendido de cable de fibra óptica o en su defecto cable UTP como cableado de backup entre equipamiento activo, con lo que se cumpla el modelo de red establecido, así también es necesario que se valide que todos los enlaces de conexión principales de fibra óptica se encuentren operando satisfactoriamente para evitar pérdidas de paquetes y reducción del rendimiento en la red.
- Teniendo en cuenta que el modelo manejará enlaces redundantes es necesario que se maneje MSTP para evitar tormentas de broadcast en la red.

#### 4.5.3.2 Nivel de acceso

Este nivel se encarga básicamente de brindar conectividad hacia el usuario final integrando todos los equipos de red finales como computadores, impresoras de red, teléfonos IP, cámaras IP, entre otros; así también en este nivel se controlan los equipos que se conectan a la red.



**Figura 19. Nivel de acceso**  
Fuente: Javier Espinosa

En este nivel es importante que se manejen aspectos referentes a:

- **Facilidad de la conexión de los dispositivos de nodo final a la red:** a fin de que sea transparente para el usuario final y para las aplicaciones que se encuentran en este nivel.
- **Manejo de VLAN:** son un componente importante en redes convergentes, éstas permiten segmentar los dominios de broadcast, aumentar ancho de banda y brindar mayor seguridad. Los switches de la capa de acceso deben permitir establecer las VLAN para los dispositivos de nodo final en la red.
- **Velocidad de puerto:** se pueden considerar dos tipos de puertos Fast Ethernet y Gigabit Ethernet.
- **Agregado de enlaces:** permiten que el switch utilice múltiples enlaces simultáneamente agregando ancho de banda hasta los switches de capa distribución.
- **Listas de control de Acceso:** permiten controlar el tráfico cursante en la red.
- **Control de Acceso a la red:** utilizado para indicarle al switch los dispositivos que se pueden conectar a la red. Este tipo de seguridad de puerto se aplica en el nivel de acceso de manera que sea la primera línea de defensa para la red. La tecnología 3Com permite realizarla basada en:
  - Dirección MAC
  - Dirección MAC y dirección IP.

- **PoE:** de ser necesario se puede considerar que los switches soporten Power Over Ethernet (PoE). Se debe tener en cuenta que el switch HP 2910 LA soporta PoE, el cual al momento no se encuentra conectado de manera óptima, por lo que se recomienda que la conexión con la capa de distribución se realice por los puertos 7 y 8 (con redundancia) que son auto negociables y las salidas para los AP o futuras implementaciones de una red wireless se utilicen los puertos del 1 al 6. Además se recomienda para este equipo la adquisición del 3Com Wireless LAN Controller WX4400, que permitiría crear una red inalámbrica, administrar y gestionar la misma.
- **QoS:** la red se debe preparar para que sea convergente y admita tráfico de red de datos, voz y video, para lo cual los switch de capa de acceso necesitan admitir QoS para mantener la prioridad del tráfico. (Por ejemplo el tráfico de voz sobre el de datos).

#### 4.5.3.2.1 Consideraciones de diseño

- Dentro del diseño se ha considerado la segmentación a nivel lógico de la red. Con el levantamiento de información realizado previamente, se ha verificado que los usuarios se encuentran agrupados en función de bloques y más no en base a funciones y los recursos que comparten, esto ha conllevado problemas relacionados a la densidad del equipamiento activo y un elevado flujo de tráfico. Esta distribución no permite la movilidad de los usuarios en función de la VLAN sino más bien los usuarios deben adaptarse hacia el bloque al cual son

redirigidos ocasionando cambios bruscos en la red y a nivel de usuario final; dificultando la escalabilidad a nivel de red.

- Teniendo en cuenta que para tener un control de la infraestructura de red, es importante asegurar que cada usuario tenga una dirección IP asignada, la misma que no sea cambiada sin previa autorización; para subsanar los posibles inconvenientes en la gestión y administración de la red se utilizará **Access management** a nivel de puerto de manera que se restrinja el uso de la red a un determinado usuario haciendo referencia a la dirección MAC y dirección IP del equipo; si uno de los dos parámetros falla el equipo no podrá conectarse a la red.
- Considerando los constantes cambios que se realizan en la infraestructura de red es necesario actualizar los diagramas de topología y documentación siempre que exista un cambio en la misma, teniendo en cuenta:
  - Interconexión de los switches y el puerto del switch que interconecta los dispositivos.
  - Rutas redundantes o los puertos agregados entre los switches que aportan rendimiento.
  - Identificación de las nuevas variantes de configuración en los switches.
  - Actualización de la información acerca de las densidades de puertos de los dispositivos y de las comunidades de usuarios (grupos de usuarios).

- Cambio o asignación de puertos del equipamiento activo y usuarios finales.
- Puertos del equipamiento activo con control de acceso a la red.

Contando con la información actualizada sobre el estado de la red, de existir problemas se podría identificar visualmente los potenciales cuellos de botella al evaluar el tráfico u otros problemas asociados en función de las áreas de servicio permitiendo brindar una solución oportuna sin afectar a toda la red.

- Una solución para evitar los switches en cascada es aplicar apilamiento, éste tipo de solución permite:
  - Operación con efectividad como un único switch más grande.
  - El uso de conexiones cruzadas de manera que la red pueda recuperarse rápidamente si falla un único switch.
  - Utilización de un puerto especial para las interconexiones de forma que no se utilice puertos de línea para las conexiones inter-switches.
  - Velocidades más rápidas de conexión de switches.
  - Convenientes cuando la tolerancia a fallas y la disponibilidad de ancho de banda son críticas y resulta costoso implementar un switch modular.

El Apilamiento es una tecnología propietaria de 3Com denominada XRN. La tecnología XRN se administra como una sola unidad, con toda la conmutación y el enrutamiento distribuido entre los múltiples dispositivos (switches).

Las ventajas que se obtiene al utilizar este tipo de tecnología son:

- **Alto rendimiento:** Una red que usa tecnología XRN puede usar múltiples switches Gigabit Capa 3 para escalar el rendimiento y la densidad de los puertos. La tecnología XRN también soporta Agregación de Enlaces (Link Aggregation) por todo el Fabric Distribuido, incrementando tanto el rendimiento como la disponibilidad.
- **Escalabilidad:** Si existe una ampliación de la cantidad de puertos en cualquier bloque se puede aumentar unidades adicionales sin reducir el rendimiento de la red.
- **Simplicidad de administración:** Fácil administración debido a que los switches apilados son administrados como una sola unidad, con una sola dirección IP, una sola configuración y sus configuraciones son sencillas de realizarlas.
- **Flexibilidad:** Varios tipos de switches Gigabit Capa 3 de 3Com soportan la tecnología XRN. Esto brinda la capacidad de mezclar y combinar diferentes medios y configuraciones de puertos en una sola unidad.

Como requerimiento para apilar switches 3Com debe tenerse en cuenta que utilicen la misma versión de Sistema Operativo y además usen el mismo sysname. El número máximo de switch que pueden apilarse es 8.

#### **4.5.4 SEGMENTACIÓN Y DIRECCIONAMIENTO IP**

Dentro de los parámetros de diseño de la red de datos se considera la seguridad en el tráfico cursante entre cada una de las redes. Una segmentación a nivel lógico basada en VLAN además de brindar seguridad limita los dominios de broadcast presentes en la red, simplifica su administración y gestión al contar con una mejor organización de la red.

##### **4.5.4.1 Segmentación y Direccionamiento IP para el nivel de Acceso**

Partiendo del levantamiento de red a nivel de usuarios, funciones y departamentos, uso de recursos y el Orgánico Funcional vigente de la institución, se ha segmentado la red en grupos o VLAN. Su distribución de manera gráfica se puede observar en la figura 56, en la cual se ilustra cada una de las subredes con un color diferente; además se puede notar que algunas de las subredes pertenecen a más de un bloque lo cual indica la asociación de los usuarios independiente de su ubicación física en la red. En el diseño se propone la creación de 16 VLAN determinadas según los departamentos y necesidades de red, considerándose además un margen de crecimiento pensando en el incremento futuro de usuarios en la red para cada una de las VLAN.

La asignación del direccionamiento IP para cada una de las VLAN está basado en un direccionamiento eficiente VLSM, el cual permite la asignación utilizando una máscara variable optimizando el uso de la redes determinadas para la institución, la asignación del direccionamiento se lo ha realizado comenzando con los grupos con mayor densidad de usuarios, hasta terminar con los grupos con menor cantidad de usuarios. Teniendo en cuenta las redes asignadas hacia la institución se las ha utilizado de la siguiente manera:

- 10.10.20.0 - utilizada para la red de servidores y equipos.
- 10.10.19.0
- 10.10.18.0
- 10.10.17.0 - redes disponibles
- 10.10.16.0
- 10.10.15.0
- 10.10.14.0
- 10.10.13.0 - utilizada para la red wireless.
- 10.10.12.0
- 10.10.11.0 - utilizadas para la segmentación de la red interna.
- 10.10.10.0
- 10.10.9.0

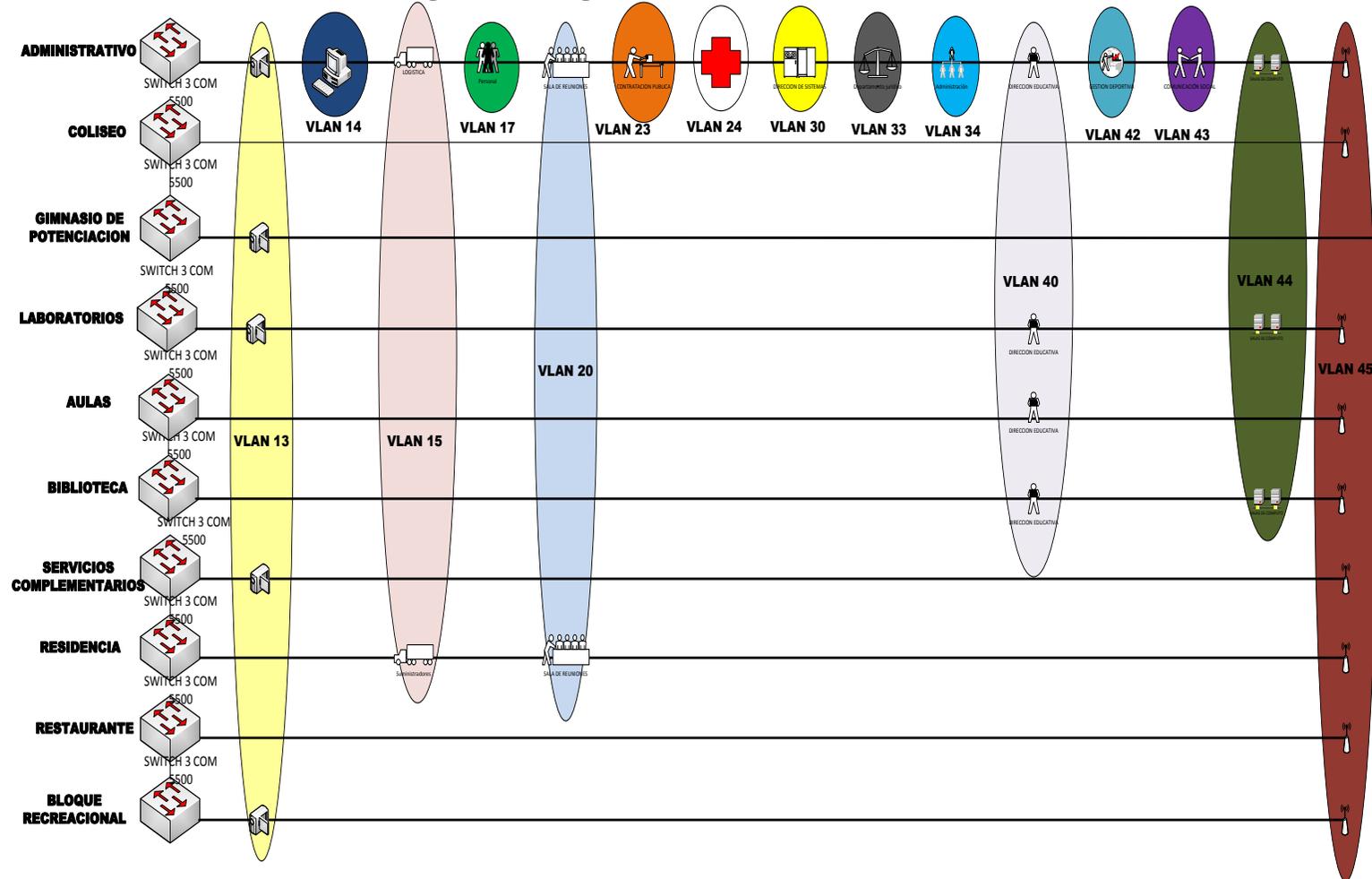
En la tabla 21 se puede observar la distribución del direccionamiento IP aplicado en función de cada una de las VLAN creadas, junto con su respectiva máscara de red, puerta de enlace y ubicación.

Tabla 16

VLAN	DEPENDENCIA	NOMBRE	# DE PUNTOS DE RED	# DE PUNTOS +50%	MASCARA DE RED	DIRECCIONAMIENTO IP	GATEWAY	LOCALIZACION BLOQUES
VLAN 1	SERVIDORES Y EQUIPOS	SRVEQ	16	24	/27	10.10.20.0 - 10.10.20.127	10.10.20.1	DATA CENTER
VLAN 13	DIRECCION ADMINISTRATIVA Y SEGURIDAD	SEGU	16	24	/27	10.10.11.160 - 10.10.11.190	10.10.11.161	B1,B3,B7,B10
VLAN 14	CUARTO DE CONTROL	CCTRL	2	3	/29	10.10.11.96 - 10.10.11.111	10.10.11.97	B1
VLAN 15	DIRECCION LOGISTICA	DIRLOGI	5	8	/29	10.10.9.192 - 10.10.9.223	10.10.9.193	B1,B8
VLAN 17	DIRECCION DE PERSONAL	DIRPER1	4	6	/29	10.10.10.0 - 10.10.10.31	10.10.10.1	B1
VLAN 20	SALAS DE REUNIONES	SREU	2	3	/29	10.10.9.0 - 10.10.9.63	10.10.9.1	B1,B8
VLAN 23	CONTRATACION PUBLICA	CONPUB	2	3	/29	10.10.11.208 - 10.10.11.223	10.10.11.209	B1
VLAN 24	SANIDAD MEDICO	SANIDAD	8	12	/28	10.10.9.224 - 10.10.9.255	10.10.9.225	B1
VLAN 30	DIRECCION DE SISTEMAS	ADMIN	3	5	/29	10.10.12.64 - 10.10.12.71	10.10.12.65	B1
VLAN 33	DEPARTAMENTO JURIDICO	JURIDICO	2	3	/29	10.10.11.80 - 10.10.11.95	10.10.11.81	B1
VLAN 34	JEFATURA ADMINISTRACION GENERAL	JEFATURA1	4	6	/29	10.10.10.192 - 10.10.10.223	10.10.10.193	B1
VLAN 40	DIRECCION EDUCATIVA	DOCTRINA	22	33	/26	10.10.12.0 - 10.10.12.40	10.10.12.1	B4,B5,B6
VLAN 42	GESTION DEPORTIVA	FED DEP	8	12	/28	10.10.11.144 - 10.10.11.159	10.10.11.145	B1
VLAN 43	COMUNICACIÓN SOCIAL	COMSOS	2	3	/29	10.10.12.48 - 10.10.12.63	10.10.12.49	B1
VLAN 44	SALAS DE COMPUTO	DIRINV	60	90	/25	10.10.11.0 - 10.10.110	10.10.11.1	B4,B6
VLAN 45	RED WIRELESS	WIRELESS			/24	10.10.13.0 - 10.10.13.255	10.10.13.1	B1,B2,B4,B5, B6,B7,B8,B9, B10

Fuente: Javier Espinosa

Figura 20. Segmentación de la red en Vlan.



Fuente: Javier Espinosa

Dentro de la distribución de VLAN se pueden diferenciar seis clasificaciones de la siguiente manera:

- **VLAN de Servidores y Equipos (SRVEQU):** es utilizada para el direccionamiento IP de la granja de servidores de aplicación de la Institución y el equipamiento activo.
- **VLAN de Administración (ADMIN):** subred perteneciente netamente a los administradores de red, únicamente los usuarios contenidos en esta subred tienen acceso a la administración del equipamiento activo.
- **VLAN de Salas de Reuniones (SREU):** esta subred contiene las salas de reuniones de cada uno de los diferentes bloques, en las mismas que a más de realizarse reuniones de las diferentes direcciones, se realizan capacitaciones por lo cual estas deben estar aisladas del resto de la red.
- **VLAN para la red Wireless (WIRELESS):** subred utilizada para la red Wireless de la Institución, la misma que por motivos de seguridad deberá permanecer aislada del resto de la red.
- El resto de las VLAN asignadas pertenecen a los diferentes grupos de usuarios.
- La declaración de las VLAN asignadas para el complejo se realizará en el switch 3Com serie 7700, el mismo que como se explicó realizará el enrutamiento INTERVLAN; a nivel de acceso se configurará las VLAN en los switch 3com de la serie 5500, los cuales brindarán la

conexión hacia el usuario final, cada uno de los puertos serán configurados según la VLAN asociada al usuario.

- Existen 4 departamentos que de acuerdo al modelo de gestión propuesto es necesario su creación como son: Contratación Pública, Dirección de Sistemas, Departamento Jurídico y Comunicación Social a los cuales se van a asignar Vlans para su correcto funcionamiento.
- Dentro del departamento de contabilidad es necesario la implementación del Sistema integrado de Gestión administrativa y financiera para el funcionamiento como empresa pública a lo cual se necesita un canal dedicado directo con el Ministerio de Economía el mismo que provee equipos de conectividad y seguridad biométricos para su funcionamiento.

#### **4.5.4.2 Listas de Control de Acceso**

Una lista de control de acceso (ACL) es utilizada para identificar flujos de tráfico, la cual al filtrar los paquetes de datos permite o deniega el tráfico cursante, de manera que se limite el tráfico en la porción de red requerida. Una ACL puede clasificar los paquetes basándose en una serie de condiciones como por ejemplo: en función de una dirección origen, dirección de destino, protocolo o puertos. Las listas de control de acceso en la tecnología 3Com están clasificadas en cuatro grupos:

- ACL Básica (numeradas del 2000 a 2999): basadas en la dirección origen.

- ACL Avanzada (numeradas del 3000 a 3999): basadas en la dirección de origen, dirección de destino, protocolo, número de puerto y otros parámetros específicos.
- ACL de capa 2 (numeradas del 4000 a 4999): basadas en campos de la cabecera de protocolo de capa 2, como dirección MAC origen, dirección MAC destino, prioridad 802.1p, y el tipo de protocolo de capa enlace.
- ACL definida por el usuario (numeradas del 5000 a 5999): basadas en información personalizada de los encabezados de protocolo.

Dentro de la clasificación de las listas de acceso las opciones más utilizadas son las ACL básicas y ACL avanzadas en los equipos de nivel de acceso. Las listas de acceso creadas pueden ser aplicadas tanto para el tráfico de entrada “inbound”, como para el tráfico de salida “outbound”, dependiendo de la aplicación que se le desee dar. Con el objeto de limitar el tráfico cursante en la red, en la institución se sugiere dos grupos de ACL diferentes:

- **Listas de acceso básicas (2800 y 2900):** utilizadas para limitar el tráfico generado por las diferentes redes.
- **Lista de acceso avanzada (3800):** utilizadas para limitar la administración del equipamiento activo a la VLAN de Administradores.
- Estas listas de control de acceso serán configuradas en los switch 3com de la serie 5500 en el nivel de acceso.

#### **4.5.4.2.1 Lista de control de acceso básica 2800**

La función de la ACL 2800 será negar el tráfico de todas las redes internas, utilizadas en el edificio. Las reglas de la lista de acceso deben ser configuradas en los puertos trunk de cada uno de los switch de bloque, ya que por medio de este puerto se encamina todo el tráfico generado. La lista de acceso 2800 es una lista de acceso básica ya que netamente será la encargada de negar el tráfico generado en la red. Con las reglas aplicadas en la lista de acceso 2800 en primera instancia se encuentra negado todo el tráfico proveniente de las redes asignadas. De no crear alguna regla para permitir el tráfico en alguna de las subredes, las máquinas de los usuarios no tendrían conexión con ninguna de las demás subredes, ni con los miembros de la misma subred.

#### **4.5.4.2.2 Lista de acceso 3800**

La función de la lista de acceso 3800 será permitir que se genere tráfico entre los miembros de una VLAN. De igual forma que la lista de acceso 2800, las reglas pertenecientes a la lista de acceso 3800 se las configurará en los puertos trunk de cada uno de los switches de acceso. A diferencia de las reglas de acceso 2800, estas deben ser configuradas dependiendo de su necesidad, es decir simplemente las subredes que estén configuradas en el switch, su asignación está dada en función de la regla asociada a cada una de las VLAN como se observa a continuación en la tabla 22:

**Tabla 17. Asignación de ACL en función de la VLAN**

VLAN	DEPENDENCIA	NOMBRE	NUMERO ACL	LOCALIZACION BLOQUES
VLAN 1	SERVIDORES Y EQUIPOS	SRVEQ		DATA CENTER
VLAN 13	DIRECCION ADMINISTRATIVA Y SEGURIDAD	SEGU	REGLA 1	B1,B3,B7,B10
VLAN 14	CUARTO DE CONTROL	CCTRL	REGLA 2	B1
VLAN 15	DIRECCION LOGISTICA	DIRLOGI	REGLA 3	B1,B8
VLAN 17	DIRECCION DE PERSONAL	DIRPER1	REGLA 4	B1
VLAN 20	SALAS DE REUNIONES	SREU	REGLA 5	B1,B8
VLAN 23	CONTRATACION PUBLICA	CONPUB	REGLA 6	B1
VLAN 24	SANIDAD MEDICO	SANIDAD	REGLA 7	B1
VLAN 30	DIRECCION DE SISTEMAS	ADMIN	REGLA 8	B1
VLAN 33	DEPARTAMENTO JURIDICO	JURIDICO	REGLA 9	B1
VLAN 34	JEFATURA ADMINISTRACION GENERAL	JEFATURA1	REGLA 10	B1
VLAN 40	DIRECCION EDUCATIVA	DOCTRINA	REGLA 11	B4,B5,B6
VLAN 42	GESTION DEPORTIVA	FED DEP	REGLA 12	B1
VLAN 43	COMUNICACIÓN SOCIAL	COMSOS	REGLA 13	B1
VLAN 44	SALAS DE COMPUTO	DIRINV	REGLA 14	B4,B6
VLAN 45	RED WIRELESS	WIRELESS	REGLA 15	B1,B2,B4,B5, B6,B7,B8,B9, B10

**Fuente: Javier Espinosa**

Adicionalmente a las reglas que permiten el tráfico entre los miembros de las VLAN, se debe crear una regla que permita el acceso a la Administración del equipamiento activo a la red de Administradores.

#### 4.5.4.2.3 Lista de acceso básica 2900

Esta lista de acceso limitará el acceso remoto para la administración del equipamiento activo a la VLAN de los Administradores, a todas las demás redes se negará su acceso. Esta lista de acceso debe ser configurada en la interface vty de cada switch.

#### 4.5.5 MANEJO DE USUARIOS Y CONTRASEÑAS

Para la administración de los switches es importante definir los niveles de acceso para los usuarios, la tecnología 3Com cuenta con cuatro niveles:

- **Nivel 0 (Visit)**

En este nivel se incluye comandos para realizar el diagnóstico de la red (como ping y traceroute), comandos para cambiar el idioma en la interfaz de usuario (language-mode) y el comando telnet. Este nivel no permite guardar los cambios de configuración.

- **Nivel 1 (Monitor)**

Este nivel se permite comandos para monitoreo (display), obtener información y eventos del sistema (debugging) y realizar diagnósticos de las fallas de servicio. Este nivel tampoco permite guardar configuraciones.

- **Nivel 2 (Manager)**

Este nivel permite usar comandos para enrutamiento y comandos de la capa de red, y se utilizan para proporcionar servicio de red directo al usuario. Este nivel permite guardar modificaciones y configuraciones. No permite crear usuarios.

- **Nivel 3 (Administrator)**

Los comandos en este nivel son los que influyen en el funcionamiento básico del módulo de apoyo del sistema, que desempeña un papel de apoyo de los servicios. Los comandos en este nivel incluyen comandos del sistema de archivos, comandos FTP, comandos TFTP, descarga de comandos XModem, comandos

de administración de usuarios, y los comandos de propiedades de nivel.

Cuando el equipamiento es nuevo, las contraseñas son las utilizadas por defecto por la tecnología utilizada y lo primero que se debe hacer es cambiarlas por motivos de seguridad y administración.

Es importante definir primeramente que usuarios van a tener acceso al equipo para asignarle un nivel y posteriormente la contraseña.

Para que la seguridad funcione adecuadamente se deben crear políticas y lineamientos de seguridad a nivel internos y capacitar al personal para hacerlas cumplir.

## **5 CAPITULO V. SIMULACIÓN DEL DISEÑO DE TOPOLOGÍA LÓGICA DE LA RED DE DATOS DEL CENTRO DE ENTRENAMIENTO PARA EL ALTO RENDIMIENTO DE CARPUELA.**

### **5.1 SIMULACIONES**

Para el desarrollo de las simulaciones que justifiquen el funcionamiento del diseño propuesto, se ha utilizado un simulador presente en el Mercado denominado Packet Tracer propietario de Cisco, dado que no existen simuladores para la tecnología 3Com que soporten las funcionalidades a demostrarse en el mismo. Packet Tracer es una herramienta utilizada con objetivos educativos que permite realizar simulaciones de manera interactiva.

La versión utilizada es 5.3.1, la misma que entre sus mejoras incluye switches capa 3 necesarios para la realización de las simulaciones.

Al inicio de éste capítulo se muestran las configuraciones realizadas en equipamiento marca 3Com, dado que el equipamiento utilizado en la Institución es de dicha marca; sin embargo en esta parte se indicarán las principales configuraciones realizadas en tecnología cisco con la cual se demuestre la funcionalidad del modelo propuesto.

Como se muestra en el desarrollo de las simulaciones, la sintaxis utilizada por ambos fabricantes es distinta, sin embargo la funcionalidad es la misma.

Cabe destacar que en lo que respecta a seguridad a nivel de acceso a la red, los fabricantes manejan una lógica diferente para cada caso.

En vista de que en la primera parte de éste capítulo se realizó un análisis de las configuraciones por cada una de las capas de manera que se tenga clara la funcionalidad de cada una de ellas junto a las configuraciones para cada caso en tecnología 3Com, en esta parte se describirá las configuraciones realizadas según aplique para cada equipo en las diferentes capas, pero no se volverá a explicar su funcionalidad ya que como se indicó anteriormente la sintaxis es la que cambia pero el objetivo de las configuraciones realizadas están dadas en base a un mismo fin.

Dentro de los equipos que ofrece el simulador cisco se tienen adicional a switches genéricos, los switches serie 2950, 2960 y 3560. Los switches 2950 y 2960 son equipos de capa 2, brindan seguridad a nivel de puerto, manejan un número máximo de vlan de 255, puertos Fast Ethernet y Giga Ethernet, soporte de LACP y ACL basadas en puertos. En cambio el switch 3560 es un switch capa 3, puertos Fast Ethernet y Giga Ethernet, soporta RSTP, PVRSTP, soporte de vlans, Soporte de PoE, LACP, Enrutamiento estático y Dinámico, Ruteo intervlan y manejo de ACL.

Dado que estos equipos brindan las características necesarias para la realización de la simulación del diseño propuesto los mismos serán

utilizados en función del modelo diseñado. Una síntesis de las características de los modelos de equipos Cisco se muestra a continuación:

**Tabla 24. Características equipamiento Cisco**

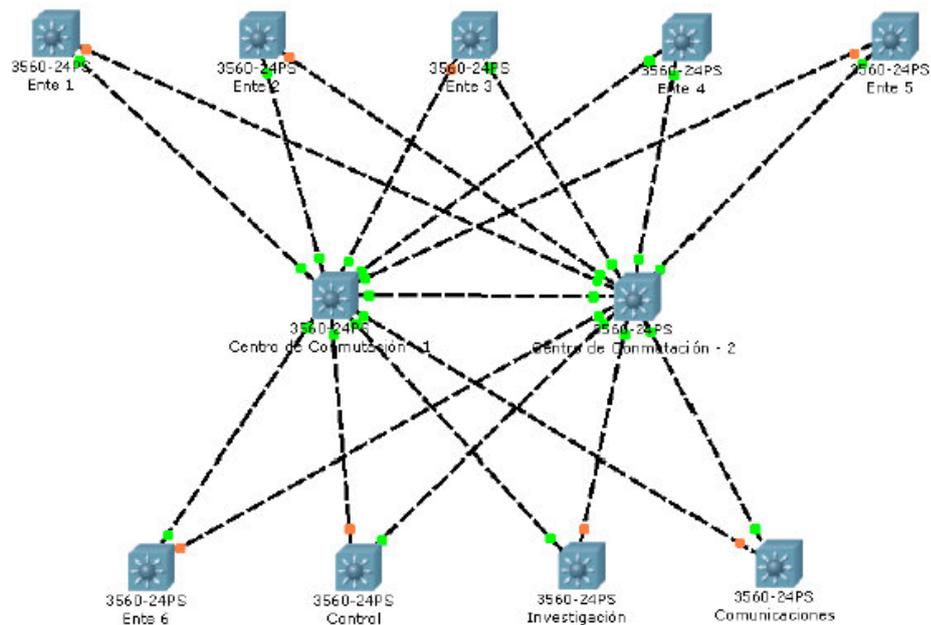
Características	Switch CISCO 2960	Switch CISCO 3560
Seguridad a nivel de puerto	X	X
Puertos Gigabit Ethernet	2	2
Puertos Fast Ethernet	24	24
Soporte de RSTP		X
IEEE 802.1.Q	X	X
Capacidad de Capa 2	X	X
Capacidad de Capa 3		X
Soporte de PoE	X	X
Manejo de ACLs	X	X
Enrutamiento Estático		X
Enrutamiento Dinámico OSPF		X
Soporte SNMP	X	X
Stacking	X	X
Switch Modular	-	-
Soporte para Agregado de Enlaces	X	X
Fuentes de poder Redundantes	-	-

**Fuente: Javier Espinosa**

### 5.1.1 TOPOLOGÍAS DE RED

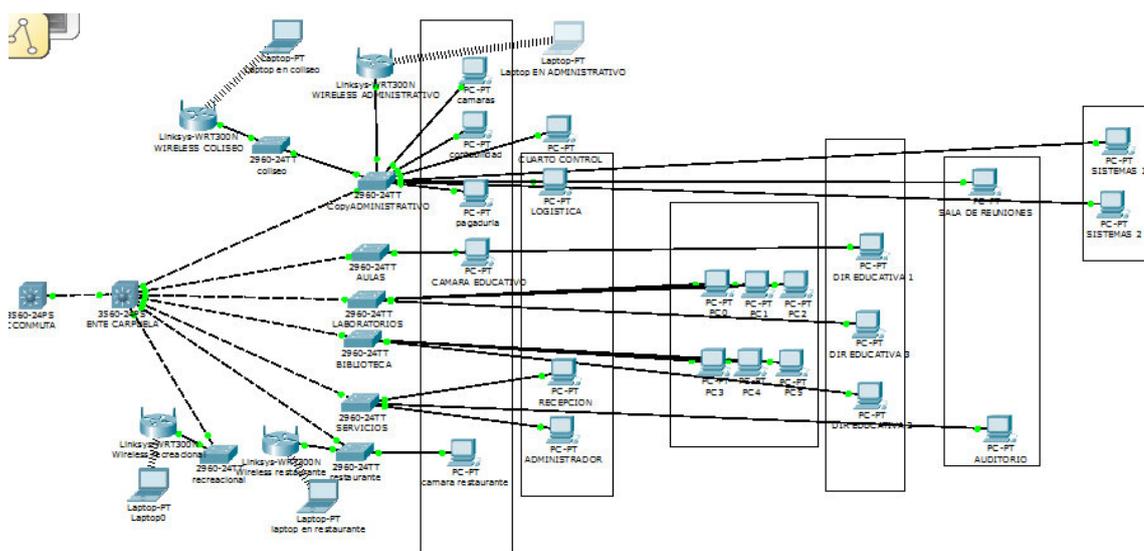
La topología que se muestra a continuación, muestra los criterios aplicados para brindar alta disponibilidad a la red, con la utilización de dos equipos robustos manejados a nivel de núcleo. Cada uno de los demás equipos simulan el equipamiento utilizado para cada uno de los Centros de entrenamiento. Para cada uno de los diferentes entes se manejan dos enlaces, cada uno de ellos está conectado hacia uno de los switches de núcleo, en los cuales a su vez se utiliza el protocolo Spanning Tree para evitar que se produzcan lazos en la red. Con la topología mostrada se tiene

un esquema “HA” dado que si un enlace falla automáticamente el enlace secundario tomará el control permitiendo que la red siga operativa.



**Figura 22. Topología en Alta Disponibilidad**  
**Fuente:** Software Packet Tracer version 5.3.1.

La figura muestra la configuración de las diferentes vlan tanto a nivel de distribución como a nivel de núcleo de manera que se limita los dominios de broadcast en la red. Además en el mismo se han implementado políticas de seguridad para el control de acceso hacia el equipamiento activo.



**Figura 23.. Topología de la red de datos de la Institución**  
**Fuente:** Software Packet Tracer version 5.3.1

Para el desarrollo de las configuraciones se tomó como base los datasheet del equipamiento.

### 5.1.2 CONFIGURACIONES BÁSICAS

En los equipos con tecnología cisco se manejan tres modos de comandos: el modo exec de usuario identificado por el carácter “>”, el modo exec privilegiado identificado por el carácter “#” y el modo de configuración que se habilita mediante el comando “configure terminal” dentro del cual se permite configurar el equipamiento.

En función del modo en el cual se trabaje se manejan diferentes niveles de acceso.

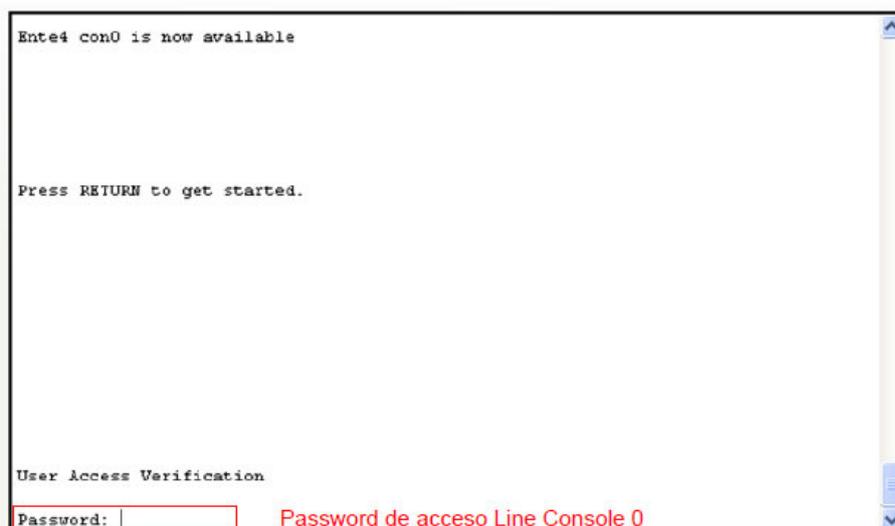
#### 5.1.2.1 Configuración de contraseñas de acceso

Dado que con el modo exec privilegiado se permite realizar cambios en la configuración, es necesario que éste sea protegido por una contraseña de

acceso. Así también para proteger el acceso hacia el equipamiento de red se deben configurar las contraseñas para el acceso a la consola y el acceso telnet habilitado por defecto. Para establecer la contraseña de consola escribir lo siguiente:

- Line console 0
- Password contraseña
- Login

Una vez establecida la contraseña para la línea de consola, para acceder a la misma se pedirá la contraseña de acceso, como se muestra a continuación:



### Habilitación contraseña de Línea de Consola

**Fuente:** Configuración equipos - Software Packet Tracer version 5.3.1

Para establecer la contraseña para modo exec privilegiado escribir:

- Enable secret contraseña .



### Habilitación modo EXEC privilegiado

**Fuente:** Configuración equipos - Software Packet Tracer version 5.3.1

Esta contraseña por defecto se almacenará cifrada Configuración password de acceso modo privilegiado .

```
Current configuration : 1774 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Bloquel
!
enable secret 5 $1$mERr$FUdo6RM3HT0HLbKYon69g0
!
!
!
!
interface FastEthernet0/1
 switchport trunk allowed vlan 1,11-16
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 13
 switchport mode access
--More--
```

Configuración password de acceso  
modo privilegiado

### Vista almacenamiento contraseña modo EXEC privilegiado

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

Para establecer la contraseña para accesos por el terminal virtual telnet, seguir el siguiente procedimiento:

- Line vty 0 4
- Password contraseña
- Login

```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan41, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan42, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan43, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state
to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan44, changed state to up

Ente4#telnet 10.10.20.2
Trying 10.10.20.2 ...Open ***ACCESO RESTRINGIDO - SOLO PERSONAL AUTORIZADO***

User Access Verification

Password: Password de acceso VTY
Bloquel>

```

### Habilitación contraseña acceso VTY

**Fuente:** Configuración equipos - Software Packet Tracer version 5.3.1

En la siguiente figura se muestra el detalle de las configuraciones realizadas:

```

interface Vlan16
  description Dep_Control
  no ip address
  !
  banner motd ^C ***ACCESO RESTRINGIDO - SOLO PERSONAL AUTORIZADO*** ^C
  !
  line con 0
    password canalelujo Password de acceso Línea de Consola 0
    login
  !
  line vty 0 4
    password szxe001 Password de acceso VTY
    login
  line vty 5 15
    login
  !
  !
end

Bloquel#

```

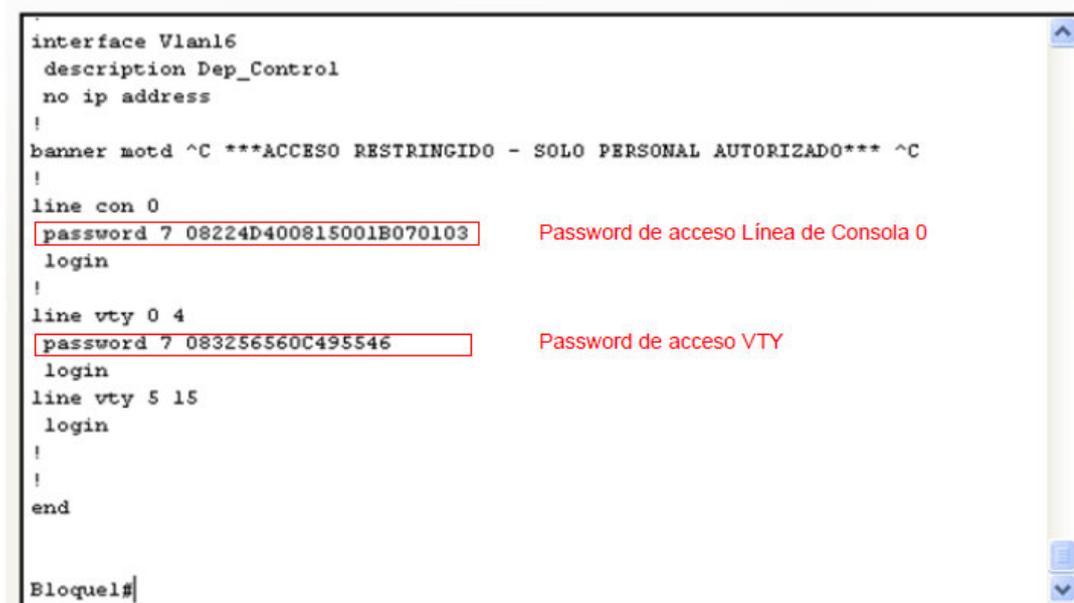
### Vista Configuración de contraseñas de acceso

**Fuente:** Configuración equipos - Software Packet Tracer version 5.3.1

Es importante tener en cuenta que las contraseñas de acceso creadas no se guardan de manera cifrada por lo cual se debe utilizar la siguiente línea de configuración:

- Service password-encryption

Una vez aplicado el comando antes indicado las contraseñas se almacenarán de manera cifrada, como se muestra en la siguiente figura:



```
interface Vlan16
  description Dep_Control
  no ip address
  !
  banner motd ^C ***ACCESO RESTRINGIDO - SOLO PERSONAL AUTORIZADO*** ^C
  !
  line con 0
  password 7 08224D400815001B070103      Password de acceso Línea de Consola 0
  login
  !
  line vty 0 4
  password 7 083256560C495546          Password de acceso VTY
  login
  line vty 5 15
  login
  !
  !
end
Bloquel#
```

#### **Vista de configuración de contraseñas de acceso cifradas**

**Fuente:** Configuración equipos - Software Packet Tracer version 5.3.1

#### **5.1.2.2 Configuración de la dirección IP del equipo**

La configuración de la dirección IP del equipo permite administrar de manera remota al equipo. Esta configuración se la ha realizado en la vlan 90 destinada para la administración del equipamiento. El direccionamiento IP asignado para cada uno de los equipos está dado de la siguiente manera:

NOMBRE DEL EQUIPO	DIRECCION IP	MASCARA	UBICACIÓN
SW_CCONMUTA	10.51.10.49	255.255.255.248	CENTRO DE COMUNICACIÓN
SW_ENTE4	10.51.10.50 10.10.20.1	255.255.255.248 255.255.255.240	DATA CENTER CARPUELA
SW_BLOQUE1	10.10.20.2	255.255.255.240	ADMINISTRATIVO
SW_BLOQUE2	10.10.20.3	255.255.255.240	AULAS
SW_BLOQUE3	10.10.20.4	255.255.255.240	LABORATORIOS
SW_BLOQUE4	10.10.20.5	255.255.255.240	BIBLIOTECA
SW_BLOQUE5	10.10.20.7	255.255.255.240	SERVICIOS COMPLEMENTARIOS
SW_BLOQUE6	10.10.20.8	255.255.255.240	RESTAURANTE
SW_BLOQUE7	10.10.20.9	255.255.255.240	RECREACIONAL

**Tabla 25. Direccionamiento IP equipamiento activo**

**Fuente: Javier Espinosa**

Para su configuración seguir los siguientes pasos:

1. Ingreso a la interfaz de administración Vlan 90
2. Asignar la dirección IP de administración del equipo.

```

interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface Vlan1
no ip address
!
interface Vlan44
description Dir_investigaciones
no ip address
!
interface Vlan90
ip address 10.10.20.9 255.255.255.240
!
banner motd ^C ***ACCESO RESTRINGIDO - SOLO PERSONAL AUTORIZADO*** ^C

```

Dirección IP - Administración del equipo

### Configuración de la IP de administración

**Fuente:** Configuración equipos - Software Packet Tracer version 5.3.1

Luego de configurada la dirección IP en cada uno de los equipos se cuenta por defecto con el acceso remoto tipo telnet: Para su acceso se debe utilizar la contraseña configurada en el terminal vty.

### 5.1.2.3 Configuración del nombre del equipo

La definición del nombre del equipo facilita las tareas de administración del mismo, su configuración se la realiza de la siguiente manera:

- Hostname nombre\_equipo

### 5.1.2.4 Configuración de acceso SSH

Antes de habilitar el acceso SSH es necesario que se configure el nombre del equipo y se defina un nombre de dominio, lo cual servirá como base para la generación de la clave RSA.

- Configuración del nombre del dominio - ip domain-name cear.local .
  - Generación de las claves RSA - crypto key generate rsa .
1. Especificar el número de bits que se utilizarán, por defecto se encuentra establecido en 512 : 1024 .
  2. Definición del tiempo de time out de ssh .
    - ip ssh time-out 30 .
  3. Definición de los reintentos de validación permitidos .
    - ip ssh authentication-retries 2 .
  4. Definición de la versión de ssh .

- ip ssh version 2 .
5. Definición del usuario y contraseña permitidos para el acceso vía ssh y sus privilegios:
    - username root privilege 15 password canalelujo1102 .
  6. Aplicar la habilitación de ssh para el terminal virtual .
    - line vty 0 4 .
  7. Activar ssh
    - transport input ssh .
  8. Definir método de logueo.
    - login local .

```

%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan5, changed state to up

00:00:40: %OSPF-5-ADJCHG: Process 1, Nbr 10.51.10.50 on Vlan5 from LOADING to FULL, Loading Done

User Access Verification

Password:

CCONMUTA>sh ip ssh
SSH Enabled - version 2.0
Authentication timeout: 30 secs; Authentication retries: 2
CCONMUTA>

```

### Vista configuración protocolo SSH

**Fuente:** Configuración equipos - Software Packet Tracer version 5.3.1

Para validar el acceso SSH desde un PC, ingresar el nombre de usuario y la dirección IP del equipo remoto, como se muestra a continuación.



Los pasos 2 y 3 son opcionales, sirven para facilitar las tareas de administración. Luego de declaradas las vlan en el caso de los switches de núcleo y distribución se debe asignar la dirección IP de la vlan, para ello seguir los siguientes pasos.

- Ingresar a la interfaz de la vlan .
- Asignar el direccionamiento IP correspondiente .
- Asignar la descripción a la interfaz de la vlan .

Las configuraciones desarrolladas se muestran en las siguientes figuras:

```
interface Vlan2
description Ente1
ip address 10.51.10.26 255.255.255.248
!
interface Vlan3
description Ente2
ip address 10.51.10.33 255.255.255.248
!
interface Vlan4
description Ente3
ip address 10.51.10.41 255.255.255.248
!
interface Vlan5
description Ente4
ip address 10.51.10.49 255.255.255.248
!
interface Vlan6
description Ente5
ip address 10.51.10.57 255.255.255.248
!
interface Vlan7
description Ente6
ip address 10.51.10.65 255.255.255.248
!
interface Vlan8
description Control
ip address 10.51.10.73 255.255.255.248
!
interface Vlan9
description Investigacion
ip address 10.51.10.81 255.255.255.248
!
interface Vlan10
description Comunicaciones
ip address 10.51.10.89 255.255.255.248
```

**Configuración de vlan a nivel de núcleo – Sw CCONMUTA**  
Fuente: Configuración equipos - Software Packet Tracer version 5.3.1



```

!
interface Vlan1
description Unidad Ejecutora
no ip address
!
interface Vlan12
description Dep_Sist_Coma
no ip address
!
interface Vlan13
description Dir_Adm_Seguridad
no ip address
!
interface Vlan14
description Cuarto_Control
no ip address
!
interface Vlan15
description Dir_Logistica
no ip address
!
interface Vlan16
description Dep_Control

```

### Configuración de vlan a nivel de acceso – Sw Bloque1

**Fuente:** Configuración equipos - Software Packet Tracer version 5.3.1

#### 5.1.4 CONFIGURACIÓN DE PUERTOS

Una vez que se han definido las vlan correspondientes se puede asignar las mismas a los puertos que conciernan. Para esto es importante diferenciar los puertos que deben asignarse en modo trunk y los que deben asignarse en modo acceso.

- Puerto conectado hacia una PC – puerto tipo acceso .
- Puerto conectado hacia un servidor - puerto tipo acceso .
- Puerto conectado hacia otro switch con una vlan - puerto tipo acceso .
- Puerto conectado hacia otro switch con varias vlan - puerto tipo trunk .

La configuración de puertos tipo trunk está dada de la siguiente manera:

- Ingresar a la interfaz del puerto deseado .

- Designar el puerto en modo trunk .
- Seleccionar la encapsulación dot1q .
- Configurar las vlan asociadas al puerto .

La configuración de puertos tipo acceso está dada de la siguiente manera:

- Ingresar a la interfaz del puerto deseado .
- Designar el puerto en modo acceso .
- Establecer la vlan a la cual pertenece el puerto .

La configuración realizada es la siguiente:

```

!
!
!
!
Interface FastEthernet0/1
description Ente4
switchport access vlan 5
switchport mode access
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!

```

**Figura 5.17. Configuración de interfaces a nivel de núcleo - Sw CCONMUTA**

**Fuente:** Configuración equipos - Software Packet Tracer version 5.3.1

Interfaz de conexión de red Descripción de la interfaz Puerto de acceso  
asignado a vlan 5 Interfaz de conexión de red Descripción de la interfaz

Puerto en modo trunk y asignación de vlan permitidas Puerto modo acceso

Habilitación encapsulación dot1q Puerto modo trunk

<code>interface FastEthernet0/1</code>	Interfaz de conexión de red
<code>description Enlace - CCUNMU1A</code>	Descripción de la interfaz
<code>switchport access vlan 5</code>	Puerto de acceso asignado a vlan 5
<code>switchport mode access</code>	Puerto modo acceso
!	
<code>interface FastEthernet0/2</code>	
<code>switchport access vlan 5</code>	
<code>switchport mode access</code>	
!	
<code>interface FastEthernet0/3</code>	Interfaz de conexión de red
<code>description Bloque1</code>	Descripción de la interfaz
<code>switchport trunk allowed vlan 1,11-16</code>	Puerto en modo trunk y asignación de vlan permitidas
<code>switchport trunk encapsulation dot1q</code>	Habilitación encapsulación dot1q
<code>switchport mode trunk</code>	Puerto modo trunk
!	
<code>interface FastEthernet0/4</code>	
<code>description Bloque2</code>	
<code>switchport trunk allowed vlan 1,13-14,16-20,32</code>	
<code>switchport trunk encapsulation dot1q</code>	
<code>switchport mode trunk</code>	
!	
<code>interface FastEthernet0/5</code>	
<code>description Bloque3</code>	
<code>switchport trunk allowed vlan 1,15,21-25,31</code>	
<code>switchport trunk encapsulation dot1q</code>	
<code>switchport mode trunk</code>	
!	
<code>interface FastEthernet0/6</code>	
<code>description Bloque4</code>	
<code>switchport trunk allowed vlan 1,20,26-33,45</code>	
<code>--More--</code>	

### Configuración de interfaces a nivel de distribución - Sw Ente4

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

#### 5.1.5 CONFIGURACIÓN DEL PROTOCOLO OSPF

Mediante la configuración del protocolo OSPF se permite habilitar un tipo de enrutamiento dinámico, establecido como estándar en la entidad. Para su configuración se debe seguir lo siguientes pasos:

- Establecer el tipo de enrutamiento ospf
- Definir las redes que se encuentran conectadas directamente al equipo y el área a la que pertenecen

```

!
interface Vlan44
 description Dir_investigaciones
 ip address 10.10.11.1 255.255.255.224
!
interface Vlan45
 description Red_Wireless
 ip address 10.10.13.1 255.255.255.0
!
router ospf 1
 log-adjacency-changes
 network 10.10.9.0 0.0.0.255 area 0
 network 10.10.10.0 0.0.0.255 area 0
 network 10.10.11.0 0.0.0.255 area 0
 network 10.10.12.0 0.0.0.255 area 0
 network 10.10.13.0 0.0.0.255 area 0
 network 10.51.10.48 0.0.0.7 area 0
!
ip classless
!
!

```

**Configuración protocolo OSPF a nivel de distribución - Sw Ente4**  
**Fuente:** Configuración equipos - Software Packet Tracer version 5.3.1

```

description Investigacion
 ip address 10.51.10.81 255.255.255.248
!
interface Vlan10
 description Comunicaciones
 ip address 10.51.10.89 255.255.255.248
!
router ospf 1
 log-adjacency-changes
 network 10.51.10.24 0.0.0.7 area 1
 network 10.51.10.32 0.0.0.7 area 2
 network 10.51.10.40 0.0.0.7 area 3
 network 10.51.10.56 0.0.0.7 area 4
 network 10.51.10.48 0.0.0.7 area 0
 network 10.51.10.64 0.0.0.7 area 5
 network 10.51.10.72 0.0.0.7 area 6
 network 10.51.10.80 0.0.0.7 area 7
 network 10.51.10.88 0.0.0.7 area 8
!
ip classless
!
!

```

**Configuración protocolo OSPF a nivel de núcleo - Sw CCONMUTA**  
**Fuente:** Configuración equipos - Software Packet Tracer version 5.3.1

## 5.1.6 HABILITACIÓN DE ALTA DISPONIBILIDAD – PROTOCOLO SPANNING TREE

Con el protocolo spanning tree se permite crear una topología libre de bucles, esto lo realiza deshabilitando los enlaces redundantes y levantando los mismos sólo en caso de ser necesario, es decir cuando el enlace principal



## 5.2 OBJETIVOS FUNCIONALES

### 5.2.1 SEGURIDAD

**Uso de contraseñas para limitar el acceso local y remoto.**- dado que mediante al acceso a la configuración del terminal se accede a tareas de administración del equipamiento, es importante que se proteja el acceso mediante el uso de contraseñas de manera cifrada.

**Uso de contraseñas cifradas y secretas.**- en primera instancia las contraseñas para acceso local y remoto son guardadas en texto plano; el uso de contraseñas secretas y el servicio para encapsular las mismas, permite proteger las contraseñas dentro de los archivos de configuración del equipo. Además de esta manera se protegen las contraseñas ante la presencia de analizadores de tráfico.

**Limitación de accesos por el terminal virtual.**- es importante definir los usuarios que pueden acceder hacia la administración remota del equipo, de forma que solo personal autorizado (Administradores de red) pueda acceder a la misma. Con la aplicación de acl de acceso se permite o niega sesiones establecidas.

**Configuración de accesos SSH:**- como es conocido telnet no es protocolo seguro, por tal motivo es necesario establecer accesos tipo ssh de forma que se permita acceder de manera segura hacia el equipamiento de manera remota, de preferencia utilizando la versión 2.

**Restricción de SNMP mediante el uso de ACL.-** dado que para realizar el monitoreo de red hacia el equipamiento activo es necesario que se habilite SNMP en los equipos es importante que se definan las direcciones habilitadas para el acceso hacia los mismos.

**Segmentación de red.-** el aplicar microsegmentación a nivel de red permite que se manejen grupos con características y funciones similares, asegurando su conectividad y seguridad. La aplicación de microsegmentación además prepara a la red para la aplicación de seguridad a nivel de equipos dedicados para ello.

## 5.2.2 DISPONIBILIDAD

**Manejo de rutas redundantes.-** Con la habilitación de rutas redundantes y la implementación de enlaces alternos se maneja una estructura en alta disponibilidad, de manera que se asegura la continuidad del servicio, en caso de que falle un enlace al detectarse en la topología un cambio de estado, se habilita el segundo enlace. La topología con enlaces redundantes permite brindar alta disponibilidad en la red y asegurar la prestación de los servicios de red. En las figuras se muestra el caso del envío de un paquete cuando se cuenta con toda la infraestructura activa uno de los puertos del enlace se encuentra en estado de espera, cuando uno de los enlaces falla

toma el control el segundo enlace y se procede a enviar los mismos por la nueva ruta asignada para la entrega del paquete.

**Habilitación protocolo de Spanning Tree.-** La habilitación del protocolo Spanning Tree permite que se maneje una estructura en HA libre de lazos debido a que siempre se mantiene activo un canal mientras que el segundo se mantiene a la escucha.

### 5.2.3 ESCALABILIDAD

**Manejo topología jerárquica.-** La aplicación del modelo permite a la red agregar nuevos dispositivos sin que ello implique la disminución del rendimiento de la misma, el uso de un modelo jerárquico de red asegura su escalabilidad sin que se cause una degradación del servicio.

### 5.2.4 DESEMPEÑO

**Eliminación de cascadas de red.-** La utilización de apilamiento a nivel de equipos de red de la capa de acceso mejora el rendimiento de la red, al manejar como un único switch más grande, reduciendo además los dominios de broadcast generados en la misma. Así también su administración se facilita.

**Limitación de dominios de broadcast.**- el empleo de microsegmentación a nivel de red permite limitar los dominios de broadcast y mejorar el rendimiento en la misma.

**Optimización del direccionamiento IP.**- el aplicar un diseño adecuado de segmentación de red optimiza el uso de las redes asignadas hacia la institución.

**Topología de red.**- mediante el diseño de red se optimizó el uso de los recursos al ubicar el equipamiento en función de las características y necesidades de la red.

#### **5.2.5 FLEXIBILIDAD**

**Manejo de topología jerárquica.**- El diseño de un modelo aplicando una topología jerárquica permite realizar cambios, modificaciones o adiciones de equipamiento de red de manera que se adapte al crecimiento de las mismas. A nivel de una topología jerárquica el agregar equipamiento se facilita, debido a que cada una de sus capas puede crecer sin ninguna dificultad técnica, ni rendimiento a nivel de aplicación.

**Microsegmentación de red.**- permite que la red se adapte a los cambios que se produzcan en la misma independientemente de la ubicación física a la cual se asignen a los usuarios en la institución, asegurando la conectividad con los usuarios del mismo segmento de red.

## **6 CAPITULO VI. CONCLUSIONES Y RECOMENDACIONES**

En base al desarrollo del trabajo realizado, en éste capítulo se exponen las principales conclusiones y recomendaciones a tomar en cuenta para la implementación y administración de la red de Datos del complejo y de la red de complejos..

### **6.1 CONCLUSIONES**

- El desarrollo del presente proyecto permitió ofrecer al Complejo Carpuela, un modelo que optimiza el uso de la red de datos, por medio de la aplicación de la topología de red basada en una estructura jerárquica brindando características de alta disponibilidad, escalabilidad, flexibilidad además de seguridad para la misma. Así también la estructura de red permite el fácil aislamiento de segmentos en caso de presentarse problemas en alguno de ellos o por motivos de mantenimiento, permitiendo que el resto de la red continúe operando.
- Teniendo en cuenta la importancia y la necesidad del servicio brindado hacia los diferentes Centros de entrenamiento por medio de la red de Datos, la aplicación de un modelo redundante tanto a nivel de enlaces como de equipamiento hace que la red cuente con alta disponibilidad asegurándose la continuidad del servicio, tanto a nivel de red interna como externa.

- El estudio de la infraestructura de red permitió identificar a detalle las principales fortalezas y falencias de la red, mediante las cuales se determinó el modelo adecuado para cumplir los objetivos funcionales del mismo, utilizando la infraestructura de red existente en función de sus características y prestaciones.
- Mediante la certificación de puntos de red realizada en la institución se determinó el estado del cableado estructurado a nivel de recorridos horizontales, encontrándola operativa en su mayor parte. Su certificación fue de fundamental importancia dado que es necesario primero determinar el estado del canal físico para luego asegurar el canal de comunicación, permitiendo brindar el servicio de manera adecuada.
- La aplicación de microsegmentación a nivel de acceso reduce el alcance de los dominios de broadcast al segmentar la red en pequeños grupos asociados en base a funciones, roles y recursos compartidos, además brinda mayor seguridad al tener acceso simplemente entre los usuarios de la vlan y de ser el caso con usuarios que necesiten realizar tareas específicas con los usuarios de otra vlan, caso contrario el tráfico entre usuarios de diferentes vlan estará cerrado; también posee flexibilidad al permitir que los usuarios de manera independiente de su ubicación física formen parte de su vlan de acceso.

- Con el levantamiento de información realizado a nivel de usuarios, se entrega a la institución la documentación técnica que servirá de ayuda en las tareas de administración y gestión, adicionalmente el administrador contará con la información necesaria para la toma de decisiones, teniendo en cuenta que el levantamiento de información a nivel de cableado estructurado, equipamiento activo, disponibilidad de puertos y servidores es de vital importancia para el manejo de la red, operación y mantenimiento.
- La aplicación del nuevo modelo de etiquetamiento para los puntos de red permitirá al administrador de red conocer de manera exacta el número del punto de red, la ubicación en patch panel, el servicio prestado además del Bloque al cual se brinde el servicio, facilitando tareas de administración, gestión y mantenimiento de la misma.
- La aplicación de seguridad a nivel de puerto con el uso del control basado en IP y MAC Address asegura que solo las máquinas autorizadas e inventariadas dentro de la red de la institución tengan acceso hacia la red interna, además brinda al administrador el control sobre la misma dado que se evitan problemas ocasionados por el cambio o robo de direcciones IP.

- El uso de un software para monitoreo de la red permite al administrador actuar de manera proactiva ante fallos en la infraestructura, adicionalmente con la ayuda del mismo tendrá una herramienta de diagnóstico visual que le permita analizar el estado de la red y la toma de decisiones.
- La aplicación de listas de control de acceso tanto asociadas a la administración del equipamiento activo como para la restricción del tráfico cursado entre las diferentes vlan asignan seguridad a la red y permiten mejorar el rendimiento de la misma.
- La habilitación de protocolos seguros para la administración del equipo brinda mayor seguridad a la red protegiéndola ante ataques mal intencionados.
- Mediante el desarrollo de las configuraciones en equipamiento de tecnología 3Com y la simulación del modelo propuesto en un simulador del mercado se puede evidenciar que de manera independiente de la infraestructura del equipamiento que se maneje el modelo es enteramente funcional. Debiendo tenerse en cuenta que ciertas características varían en relación a la tecnología de equipamiento utilizado, sin embargo el modelo cumple con todos los objetivos funcionales dado que los criterios aplicados son los mismos.

## 6.2 RECOMENDACIONES

El personal encargado de la administración y gestión de la red debe estar actualizado y capacitado de forma continua en gestión y administración de redes además en seguridad informática para la toma de decisiones ante problemas y progresos en la red.

Para todas las instalaciones de cableado estructurado que se realicen, debe utilizarse accesorios y ductos adecuados, además de una correcta identificación, teniendo en cuenta los criterios detallados en las normas ANSI/TIA/EIA.

Se recomienda llevar una bitácora de todos los acontecimientos presentados en la red, tanto los incidentes producidos como las acciones que se tomen al respecto.

Se debe documentar todos los cambios que se realicen en la red, tanto a nivel de usuarios, enlaces, direccionamiento aplicado, vlan asignada, perfiles, entre otros, de manera que se cuente con la información actualizada y en cualquier momento se pueda tomar decisiones en base a ella. Esta documentación facilitará las tareas de administración en caso de que el personal encargado no se encuentre presente y se deba delegar funciones.

Es importante que se establezcan políticas a nivel de red de manera que se regule y controle el uso de ella y de los equipos computacionales, la

misma que luego de ser aprobada debe ser socializada a todo el personal de la institución de manera que se dé cumplimiento al mismo.

En vista de que el Data Center constituye un punto crítico en la red interna es importante que este cuente con un constante monitoreo en tiempo real, con el uso de cámaras de seguridad, además es importante contar con un monitoreo digital que alerte al administrador ante la presencia de valores anormales en el ambiente del mismo.

Para la aplicación del modelo que brinde alta disponibilidad a la red, se debe tomar en cuenta rutas diferentes para la instalación de los enlaces de conexión, de manera que de producirse falla en el recorrido del enlace, el canal alternativo no se vea afectado y se asegure la continuidad del servicio.

Se debe contar con procedimientos para el cambio periódico de contraseñas del equipamiento activo, utilizando contraseñas con un nivel de complejidad adecuado, utilizando la combinación de letras mayúsculas, minúsculas, números y caracteres especiales de manera que se brinde mayor seguridad a la misma; dentro del procedimiento deben considerarse el mecanismo para el almacenamiento bajo custodia de las contraseñas cambiadas, en caso de que las mismas sean requeridas de manera urgente y ningún personal de la sección se encuentre en el establecimiento. Estas contraseñas sólo podrán ser abiertas en situaciones extremas por el Jefe de la sección.

Se recomienda realizar backup periódicos de las configuraciones del equipamiento activo, guardando las versiones anteriores (mínimo 5), de manera que de ocurrir problemas en alguna configuración mal aplicada o corrupción de la misma se pueda subir un backup y restituir de manera inmediata el servicio. En dependencia del cambio de configuraciones a nivel de equipamiento se recomienda sacar backup semanales o quincenales dados mediante un procedimiento establecido.

Con el fin de precautelar la seguridad de la institución y tener un control sobre los equipos computacionales y el uso de los mismos, es conveniente que todos los equipos sean configurados dentro del directorio activo institucional.

El software de monitoreo debe ser constantemente revisado, además se debe tener en cuenta que cualquier cambio o adición que se realice en la infraestructura debe ser actualizado en el mismo.

Dado que el proyecto se basa en la aplicación de seguridad a nivel de red, es importante que se apliquen soluciones firewall para brindar seguridad a la red perimetral ante accesos no autorizados u ataques a la misma.

Se deben implementar esquemas técnicos de seguridad perimetral para la red de internet y de datos tales como Firewall, IDS, IPS, VPN.

Se recomienda que los puertos del equipamiento de red que no estén siendo utilizados con autorización del personal de administración sea deshabilitado, de manera que se controle y regule el uso de la red asegurando además su seguridad.

De los problemas detectados a nivel de puntos finales de cableado estructurado es importante que se trate de dar solución a los que por problemas de mal manejo o prácticas de instalación presentan fallas en el mapa de cableado en alguno de sus extremos, sin embargo los puntos de red con problemas internos del cable, de preferencia no deben ser utilizados ya que la eficiencia del enlace no está garantizada.

## 7 Bibliografía

- 3Com. (2 de Octubre de 2013). *L3 3Com*. Obtenido de <http://www.l-3com.com/>
- Armendáriz, L. M. (2009). *Cableado Estructurado*. Barcelona: Autoedición.
- Carrero, B. (5 de Abril de 2011). *Monografias.com*. Obtenido de <http://www.monografias.com/trabajos11/utp/utp.shtml>
- CCNA. (5 de Enero de 2011). *Diseño de Lan*. Obtenido de <http://pantheanet.blogspot.com/2012/01/tema-1-diseno-de-lan.html>
- Cisco Co. (14 de enero de 2005). *Router-switch Ltd*. Obtenido de [http://www.router-switch.com/Price-cisco-routers-cisco-router-800-series\\_c74?gclid=CMnWkfOry8ICFTFp7AodqhQA-A](http://www.router-switch.com/Price-cisco-routers-cisco-router-800-series_c74?gclid=CMnWkfOry8ICFTFp7AodqhQA-A)
- CNNA. (15 de Junio de 2013). *Programacion Redes CNNA*. Obtenido de <http://computopractico.blogspot.com/2009/07/212-historia-de-las-redes-informaticas.html>
- ELIE. (27 de Mayo de 2010). *Blog de Redes*. Obtenido de <http://redeselie.blogspot.com/2010/05/tipos-de-topologias-topologia-o-forma.html>
- Fluke Co. (4 de febrero de 2010). *Fluke Networks*. Obtenido de <http://es.flukenetworks.com/datacom-cabling/copper-testing/LinkWare-Cable-Test-Management-Software>
- Garcia, J. (1994). *Redes para procesos Distribuidos*. En J. Garcia. Madrid: Editorial RA-MA.
- Gerónimo, A. F. (21 de AGOSTO de 2007). *Monografias*. Obtenido de [WWW.MONOGRAFIAS.COM](http://WWW.MONOGRAFIAS.COM): <http://www.monografias.com/trabajos13/modosi/modosi.shtml>
- Hp Hewlet Packard. (2 de junio de 2013). *Switches y routers HP*. Obtenido de <http://h17007.www1.hp.com/ec/es/networking/products/switches/index.aspx>
- Jimenez, C. (6 de Enero de 2012). *Monografias*. Obtenido de <http://www.monografias.com/trabajos90/redes-interconexion/redes-interconexion.shtml>

Manyari, M. A. (27 de agosto de 2008). *Monografias.com*. Obtenido de <http://www.monografias.com/trabajos93/cableado-estructurado2/cableado-estructurado2.shtml>

McGraw-Hill, E. (11 de Noviembre de 2008). *Mailmax.com*.

Ministerio Del Deporte Ecuador. (2014). *Modelo de Gestion Definitivo CEAR EP*. Quito: Ministerio del Deporte.

SECOB Servicio de Contratacion de Obras. (15 de Octubre de 2012). *WWW.secob.gob.ec*.

TIA/EIA. (2002). *Administration Standard for Commercial Telecommunications Infrastructure*. Los Angeles CA: TIA/EIA.

## ÍNDICE DE ACRÓNIMOS

**ACL:** Access Control List (Listas de Control de Acceso)

**ACR:** Attenuation/Crosstalk Ratio (Relación Atenuación-Diafonía)

**ADSL:** Asymmetric Digital Subscriber Line (Línea de Abonado Digital Asimétrica) **AP:** Access Point (Punto de Acceso)

**ARP:** Address Resolution Protocol (Protocolo de Resolución de Direcciones)

**ARPA:** Advanced Research Proyects Agency (Agencia de Investigación de Proyectos Avanzados)

**ARPANET:** Advanced Research Proyects Agency Network (Red de la Agencia de Investigación de Proyectos Avanzados)

**ASIC:** Application-Specific Integrated Circuit (Circuitos Integrados de Aplicación Específica)

**BGP:** Border Gateway Protocol (Protocolo de Gateway de Borde)

**BITNET:** Because It's Time Network (Red Porque ya es Hora)

**BPDU:** Bridge Protocol Data Units (Unidad de Datos de Protocolo Puente)

**CE:** Cableado estructurado

**CEAR:** Centro de Entrenamiento para el Alto Rendimiento.

**CHAP:** Challenge Handshake Authentication Protocol (Protocolo de Autenticación por Desafío Mutuo)

**CNLP:** Connection less Network Layer Protocol (Protocolo de Capa de Red Sin Conexión)

**CPU:** Central Processing Unit (Unidad Central de Procesos)

**CSMA/CD:** Carrier Sense Multiple Access with Collision Detection (Acceso Múltiple por Detección de Portadora con Detección de Colisiones)

**CSNET:** Computer Science Network (Red de Ciencias de la Computación)

**DES:** Data Encryption Standard (Estándar de Cifrado de Datos)

**DHCP:** Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Host)

**DNS:** Domain Name System (Sistema de Nombres de Dominio)

**EAPOL:** Extensible Authentication Protocol Over LAN (Protocolo de Autenticación Ampliable sobre LAN)

**ECMP:** Equal-Cost Multi-Path (Igual Costo Multitrayecto)

**EIGRP:** Enhanced Interior Gateway Routing Protocol (Protocolo de Enrutamiento de Gateway Interior Mejorado)

**ELFEXT:** The Equal-Level Far-End Crosstalk (Telediafonía por igualación de Nivel) **FEXT:** Far-End Crosstalk (Interferencia de Extremo Lejano - Telediafonía)

**FTP:** Foiled Twisted Pair (Par Trenzado con Pantalla Global)

**FTP:** File Transfer Protocol (Protocolo de Transferencia de Archivos)

**HTTP:** Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto) **HTTPS:** Hypertext Transfer Protocol Secure (Protocolo de Transferencia de Hipertexto Seguro)

**ICMP:** Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet)

**IEEE:** The Institute of Electrical and Electronics Engineers (Instituto de Ingenieros Eléctricos y Electrónicos)

**IETF:** Internet Engineering Task Force (Grupo de Trabajo en Ingeniería de Internet) **IGMP:** Internet Group Management Protocol (Protocolo de Administración de Grupos de Internet)

**IGRP:** Interior Gateway Routing Protocol (Protocolo de Ruteo de Gateway Interior) **IMAP:** Internet Message Access Protocol (Protocolo de Acceso a Mensajes Internet) **IP:** Internet Protocol (Protocolo de Internet)

**IPX:** Internetwork Packet Exchange (Intercambio de Paquetes Interred)

**IS-IS:** Intermediate System - Intermediate System (Sistema Intermedio - Sistema Intermedio)

**ISM:** Industrial, Scientific and Medical (Industrial, Científica y Médica)

**ISO:** International Standards Organization (Organización Internacional de Estándares)

**ITU:** International Telecommunication Union (Unión Internacional de Telecomunicaciones)

**LACP:** Link Aggregation Control Protocol (Protocolo de Control de Agregación de Enlace)

**LAN:** Local Area Network (Redes de Área Local)

**LLC:** Control de Enlace Lógico (Logical Link Control)

**LSP:** Link State PDU (PDU de Estado de Enlace)

**MAC:** Media Access Control (Control de Acceso al Medio)

**MAN:** Metropolitan Area Network (Red de Área Metropolitana)

**MAPs:** Managed Access Points (Administración de Puntos de Acceso)

**MILNET:** Military Network (Red Militar)

**MSTP:** Multiple Spanning Tree Protocol (Protocolo Múltiple de Spanning Tree)

**NEXT:** Near-End Crosstalk (Interferencia de Extremo Cercano)

**NIC:** Network Interface Card (Tarjeta de Interfaz de Red)

**ODFs:** Optical Distribution Frame (Repartidores de Fibra Óptica)

**OSI:** Open System Interconnection (Interconexión de Sistemas Abiertos)

**OSPF:** Open Shortest Path First (Primero el Camino Libre más Corto)

**PAP:** Password Authentication Protocol (Protocolo de Autenticación de Contraseña)

**PIM SM/DM:** Protocol Independent Multicast Sparse Mode/Dense Mode (Protocolo Multicast Independiente Modo Esparcido/Modo Denso)

**PoE:** Power Over Ethernet (Poder sobre Ethernet)

**POP:** Post Office Protocol (Protocolo de la Oficina de Correo)

**PSELFEXT:** Power Sum the Equal-Level Far-End Crosstalk (Telediafonía de Suma de Potencias por Igualación de Nivel)

**PSNEXT:** Power Sum Near-End crosstalk (Paradiafonía de Suma de Potencias)

**QoS:** Quality of Service (Calidad de Servicio)

**RARP:** Reverse Address Resolution Protocol (Protocolo de Resolución de Dirección Inversa)

**RIP:** Routing Information Protocol (Protocolo de Información de Enrutamiento)

**RSN:** Robust Secure Network (Red de Seguridad Robusta)

**RSTP:** Rapid Spanning Tree Protocol (Protocolo Rápido de Spanning Tree)

**SCE:** Sistema de Cableado Estructurado

**SMTP:** Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correo) **SNMP:** Simple Network Management Protocol (Protocolo Simple de Administración de Red)

**SPF:** Shortest Path First (Primero la Ruta más Corta)

**SSH:** Secure Shell (Intérprete de Comandos Seguro)

**SSID:** Service Set Identifier (Identificador de Conjunto de Servicio)

**STP:** Shielded Twisted Pair (Par Trenzado Apantallado)

**STP:** Spanning Tree Protocol (Protocolo de Spanning Tree)

**TCP:** Transmission Control Protocol (Protocolo de Control de Transmisión)

**TCP/IP:** Transmission Control Protocol/Internet Protocol (Protocolo de Control de Transmisión/Protocolo de Internet)

**TELNET:** Telecommunication Network (Red de Telecomunicaciones)

**TIC:** Tecnologías de la Información y Comunicación

**TKIP:** Temporal Key Integrity Protocol (Protocolo de Integridad de Clave Temporal) **TSB:** Technical Service Bulletin (Boletín Técnico de Servicio)

**UDP:** Protocolo de Datagrama de Usuario (User Datagram Protocol)

**UPS:** Uninterruptible Power Supply (Fuente de Alimentación Ininterrumpible)

**UTM:** Unified Threat Management (Gestión Unificada de Amenazas)

**UTP:** Unshielded Twisted Pair (Cable Trenzado sin Apantallar)

**VLAN:** Virtual Local Area Network (Redes de Área Local Virtuales)

**VLSM:** Very Large Mask Variable (Máscara de Longitud Variable)

**WAN:** Wide Area Network (Red de Área Extensa)

**WAP:** Wireless Application Protocol (Protocolo de Aplicaciones Inalámbricas)

**WEP:** Wired Equivalent Privacy (Privacidad Equivalente por Cable)

**WIFI:** Wireless Fidelity (Fidelidad inalámbrica)

**WLAN:** Wireless Local Area Network (Redes de Área Local Inalámbricas)

**WPA:** Wifi Protect Access (Acceso Inalámbrico Protegido)

**XRN:** eXpandable Resilient Networking (Networking Redundante Expansible)