

**DISEÑO DE IMPLEMENTACION LABORATORIO DE REDES
(DILR)**

**LUIS ALEJANDRO ALONSO
DIEGO AVILA AREVALO**

**UNIVERSIDAD MINUTO DE DIOS
REDES Y SEGURIDAD INFORMATICA
SOACHA
2013**

**DISEÑO DE IMPLEMENTACION LABORATORIO DE REDES
(DILR)**

**LUIS ALEJANDRO ALONSO
DIEGO AVILA AREVALO**

**Diseño Técnico de laboratorio de Redes y Seguridad para Universidad
Minuto de Dios Centro Regional Soacha**

IVAN GARCIA

**UNIVERSIDAD MINUTO DE DIOS
REDES Y SEGURIDAD INFORMATICA
SOACHA
2013**

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Soacha día de mes del 2013

AGRADECIMIENTOS

Con orgullo y cariño le agradecemos a nuestras madres, Janeth Bernate, Hilda María Arévalo, Padres, Pablo Bernal Alonso, Jesús Antonio Ávila, a nuestros profesores que a través del proceso académico siempre estuvieron ahí apoyándonos y asesorándonos sobre como recibir el conocimiento que nos han estado aportando, como son; Julián Romero, Paola Gutiérrez, Ana Maria Obando, Ximena Sabogal, Carlos Charry, John Barcancel, y todos aquello que estuvieron ahí en cada semestre y en cada materia.

También queremos agradecer a la Universidad minuto de Dios Centro Regional Soacha, a sus coordinadores y a todas aquellas personas que nos acompañaron durante este proceso.

Atentamente,

Luís Alejandro Alonso
Diego Ávila Arévalo

CONTENIDO

Pág.

INTRODUCCIÓN

1	TEMA		
	114		
1.1.1	PLANTEAMIENTO DEL PROBLEMA		
	114		
1.1.2	DESCRIPCIÓN		15
1.1.3	FORMULACIÓN DEL PROBLEMA		15
1.1.4	ALCANCES		16
1.1.5	DELIMITACIONES		16
1.1.6	OBJETIVO GENERAL		17
1.1.7	OBJETIVOS ESPECIFICOS		17
1.1.8	JUSTIFICACION		18
1.1.9	HIPOTESIS GENERAL		18
1.1.10	HIPOTESIS DE TRABAJO		19
1.1.11	MISION		19
1.1.12	VISION		19
1.1.13	ANTECEDENTES		19
1.1.14	MARCO HISTÓRICO		20
1.1.15	MARCO LEGAL		22
1.1.16	MARCO TEORICO		24
1.1.17	ESTUDIO DE CAMPO		47
2	FASE DE INICIO		48
2.1	DESCRIPCION DE LA ESTRUCTURA FISICA		48
2.1.1	DESCRIPCION DE LA ESTRUCTURA ELECTRICA		49
2.1.2	DESCRIPCION DE LAS ZONAS COMUNES		49
2.2.1	REQUISITOS PUNTOS DE RED		49
2.2.2	REQUISITOS CRECIMIENTO FISICO DE LA RED		50
2.2.3	REQUISITOS DE SEGURIDAD FISICA		51
2.2.4	REQUISITOS LOGICOS		54
2.2.4.1	TIPO INFORMACION TRANSMITIDA POR LA RED		54

2.2.4.2	VELOCIDAD Y FLUJO DE DATOS	54
2.3.3	REQUISITOS DE SEGURIDAD LOGICA	55
3	DISEÑO DE LA RED	55
3.1.1	DISEÑO FISICO	55
3.1.2	MODULO CABLEADO	67
3.1.3	MODULO INALAMBRICO	67
3.2.1	DISEÑO LOGICO	70
3.2.2	ARQUITEDTURA DE LA RED	70
3.2.3	DIRECCIONAMIENTO IP	71
3.2.4	METODOS DE ACCESO	72
3.2.5	DIAGRAMA LOGICO DE LA RED	73
3.3	SELECCIÓN Y EVALUACION DE TECNOLOGIAS	74
3.3.1	SOFTWARE	76
4	PRESUPUESTO	80
5	CONCLUSIONES	81
6	BIBLIOGRAFIA E INFOGRAFIA	82
7	ANEXOS	83

LISTA DE TABLAS

	Pág.
Tabla 1. Equipos Activos.	83
Tabla 2. Especificaciones técnicas del servidor	84
Tabla 3. Accesorios y Herramientas	84
Tabla 4. Otros Improvistos	85
Tabla 5. Totales	85
Tabla 6. Inventario Aula 311A	86

LISTA DE FIGURAS

	Pág.
Figura 1. Backbone	91
Figura 2. Lista IEEE 802	91
Figura 3. Ejemplo Conexión Inalámbrica	92
Figura 4. Ejemplo Conexión Servidores	92
Figura 5. Topología de red	93
Figura 6. Laboratorio 311	93

LISTA DE ANEXOS

	Pág.
ANEXO I. CRONOGRAMA DE ACTIVIDADES.	94
ANEXO II. FOTOGRAFÍAS ESTUDIO DE CAMPO	96

GLOSARIO

Arpanet: (Advanced Research Projects Agency Network) primera red de computadores creada por encargo del Departamento de Defensa de los Estados Unidos como medio de comunicación para los diferentes organismos del país.

Datagrama: Forma en que se encaminan los paquetes en una red.

SMTP: Protocolo para la transferencia simple de correo electrónico.

NNTP: es un protocolo inicialmente creado para la lectura y publicación de artículos de noticias en Usenet. Su traducción literal al español es "protocolo para la transferencia de noticias en red".

Aterramiento: es un sistema eléctrico de potencia, para cubrir los sistemas de puesta a tierra y neutro.

ATM: es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

Distro: es una distribución de software basada en el núcleo Linux que incluye determinados paquetes de software para satisfacer las necesidades de un grupo específico de usuarios.

Atenuación: pérdida de potencia sufrida por la misma al transitar por cualquier medio de transmisión.

RESUMEN

Al desarrollar el análisis técnico para un laboratorio de redes y seguridad informática, lo primero que se debe tener en cuenta es el área en donde se está implementando, al ser el principal objeto de estudio por la normatividad que implica un cableado estructurado, en donde se analiza qué características se tienen en su interior, como la distribución eléctrica, si se encuentra en óptimas condiciones; así como también la humedad dentro de ella para salvaguardar el hardware y software a ser instalado y otros aspectos importantes que se irán nombrando a lo largo de este documento.

Realizando el análisis anterior y culminando apropiadamente su proceso, en el centro Regional Uniminuto Soacha, comenzara una nueva forma de estudiar las redes al tener la posibilidad de realizar las practicas conforme el plan de estudios que la institución académica expresa en su pensum y así lograr un posible objetivo en común que es el de aumentar el reconocimiento que tiene la universidad a nivel regional dando mejores expectativas a los egresados de esta carrera y otras afines que se beneficiarían de este proyecto para encontrar una mejor ubicación en el ámbito laboral al poseer el conocimiento necesario para esta etapa de sus vidas.

ABSTRACT

In developing the technical analysis to a laboratory network and computer security, the first thing you should consider is the area where it is being implemented, as the main object of study by the regulations involving structured cabling, where analyzes what features are inside such as electrical distribution if it is in good condition as well as moisture in it to protect the hardware and software to be installed and other important aspects that will be naming throughout this document.

By performing the above analysis and properly completing the process at the regional center Uniminuto Soacha, began a new way of studying the networks to be able to perform the practice as the curriculum that academy expressed in its curriculum and achieve a possible common goal which is to increase the recognition that the university has a regional giving better prospects for graduates of this and other related career that would benefit from this project to find a better location in the workplace to possess the necessary knowledge for this stage of their lives.

INTRODUCCION

Las tecnologías de la información aplicadas a la educación se están imponiendo como apoyo a los procesos de enseñanza y aprendizaje, son herramientas especializadas que permiten fortalecer desde la didáctica procesos cognitivos que desarrollan en los estudiantes capacidades para comprender e interpretar, por esta razón es necesario estudiar las condiciones de calidad con el fin de proponer estrategias de apoyo a los procesos de la enseñanza reafirmando conocimientos como Tecnólogos en redes y seguridad informática, para alcanzar la primer meta planteada en este proceso de crecimiento intelectual en el que se esta envuelto actualmente, dando así origen al diseño del laboratorio de redes y seguridad informática, y su plan de implementación para la Universidad Minuto de Dios Centro Regional Soacha.

En el centro Regional Soacha es necesaria la creación de un laboratorio de redes y seguridad por su importancia en el desarrollo de las clases practicas que dan complemento al esquema de educación planteado por la institución, para que esto sea posible, se está realizando un estudio técnico para evaluar el área de implementación, y los componentes con los que la Universidad cuenta. Lo que es el objetivo de este proyecto, en donde se realizan una serie de procesos, obteniendo unos resultados finales señalando la propuesta optima de diseño según lo estudiado, dando así alternativas para la consecución de la implementación de la red, utilizando las tecnologías actuales de cableado como son fibra óptica, coaxial, inalámbrico con las normas a las cuales están sujetas dejándolo así a la vanguardia de la tecnología que hoy mueve el mundo.

Este proyecto producirá que la Universidad contemple la necesidad del laboratorio, las estrategias para su realización, y así sea posible que para el siguiente año se piense en su construcción, asegurando un futuro mejor para el proceso educativo de las próximas generaciones que estudiarían esta carrera, teniendo como valor agregado la posibilidad de realizar practicas que fortalezcan su conocimiento, dejando atrás una falencia para que se interpone con la razón de ser de estudiar en uniminuto en donde las posibilidades de aprendizaje son muy buenas por su labor social y cultural en la comunidad, con este documento se dejaría precedente de los conocimientos adquiridos enfocados a la solución de problemas y colaboración hacia la sociedad.

Para comenzar el análisis se tendrá en cuenta el área del salón en el cual se implementara el laboratorio, tendido eléctrico de este, hardware y software a instalar en el, inventario que posee la universidad dejando listo un modelo con el

cual el estudiante se sienta identificado y logre el propósito de convertirse en un especialista de las redes y la seguridad informática.

1. TEMA

Diseño tecnico del laboratorio de redes y seguridad informatica en la Universidad Minuto de Dios centro regional Soacha

1.1.1 PLANTEAMIENTO DEL PROBLEMA

En la Universidad Minuto de Dios centro regional Soacha, no se tiene un laboratorio de redes y seguridad informática adecuado para las practicas de la carrera de redes y seguridad informática, lo que es necesario, ya que las materias del programa como son, Introducción a la tecnología en Redes, Redes LAN, Redes Inalámbricas, seguridad en Redes, Redes WAN, auditoria en Redes, Hacking ético, Gestión de Redes, CPC, e informática forense, en su cronograma de actividades especifican prácticas tales como administración de redes LAN, administración de redes WAN, administración de redes inalámbricas, configuración de routers y sistema operativo (NOS), mapas de ruteo ipv4, ipv6, instalación de firewalls, antispam, medidores de seguridad y administradores de recursos tanto físicos como lógicos de Red; estos requerimientos no se pueden realizar en los laboratorios de informática por las restricciones que se tienen en las salas, lo cual genera dificultad en el buen desarrollo de las clases del programa de redes y seguridad informática.

Lo anterior nos hace recurrir a simulaciones en software, dejando vacíos al no tener las herramientas para la solución de tantos problemas que a nivel físico ocurren en el montaje de una Red y que al hacerlas en un laboratorio de redes, tendrían un aumento considerable en el aprendizaje al generar el desarrollo de la práctica y así contribuir a la formación académica con miras al campo laboral. Teniendo en cuenta los inconvenientes anteriormente mencionados, la solución que se plantea es el de diseñar e implementar un laboratorio de Redes y seguridad informática que permita a los docentes y estudiantes desarrollar todas las actividades académicas del programa de tecnología en redes y seguridad informática.

1.1.2 DESCRIPCIÓN

El egresado del programa de Redes de Computadores y Seguridad Informática, enfoca sus objetivos hacia el desempeño laboral como solucionar problemas a nivel de conexión, diseñador o administrador de redes de datos. Participa como colaborador en diferentes proyectos de redes de datos donde se requiera la implementación de soluciones en hardware ó software. Está en capacidad de proponer alternativas eficientes de solución a licitaciones u ofertas relacionadas con cableado estructurado. En el entorno académico del área el egresado puede realizar aportes importantes en proyectos de investigación.

Para cumplir a cabalidad con lo anteriormente escrito que es lo expresado por la Universidad Uniminuto este proyecto pretende hacer un análisis y un diseño técnico con las especificaciones técnicas adecuadas a los estándares nacionales, de un laboratorio de redes ya que al faltar no permite el óptimo proceso para el desarrollo del enfoque de los objetivos trazados por cada estudiante del programa.

En este proyecto se evalúa un diseño acorde con las instalaciones de la Universidad Minuto De Dios Centro Regional Soacha y se entrega para una posible implementación y pronta ejecución de los datos aquí consignados desde normas de cableado estructurado hasta planes de manejo para las practicas del laboratorio, así se ayuda a mejorar la calidad de aprendizaje de la universidad y solventa una necesidad critica que en la actualidad es demandada por los estudiantes.

1.1.3 FORMULACIÓN DEL PROBLEMA

¿Si en la Universidad Minuto De Dios Centro Regional Soacha existiera un laboratorio adecuado para ser usado en la carrera de redes y seguridad informática, será que las inconsistencias en las clases del programa académico que ofrece, disminuirían, al ofrecerle a los estudiantes métodos prácticos y un lugar adecuado para desarrollar los conocimientos infundados en esta, entrando en un aula diseñada para la mejor obtención de conocimientos prestando así mejores servicios de educación, promoviendo con esto una mayor capacidad para enfrentarse en el mundo laboral que espera a sus estudiantes?.

1.1.4 ALCANCES

El análisis técnico que se realiza para definir el proceso que se lleva a cabo registra los siguientes alcances:

- Normas cableado estructurado redes Lan, wireless
- Configuración Hardware y Software de un laboratorio
- Diseño físico Laboratorio de Redes
- Diagrama lógico de la red Lan, Wireless
- Arquitectura de la red Lan, Wireless
- Direccionamiento ip red Lan, Wireless
- Métodos de acceso de usuarios
- Requisitos Físicos red Lan, wireless
- Requisitos Lógicos Lan, wireless
- Estándares de seguridad redes Lan, wireless
- Planos laboratorio

1.1.5 DELIMITACIONES

Para delimitar el análisis del laboratorio de redes se tienen en cuenta los siguientes parámetros que son.

- Identificar las normas colombianas para el cableado estructurado
- lineamientos de uso del laboratorio según el plan de estudios de la carrera de redes y seguridad informática
- análisis de la configuración ideal del hardware para un laboratorio de redes
- Plan de implementación.
- Propuesta elementos faltantes.
- Selección de tecnologías.
- Propuesta practicas a desarrollar en el laboratorio
- Diseño técnico laboratorio redes
- Enrutamiento ipv 4
- Hardware disponible
- Planeación un solo laboratorio
- presupuesto

1.1.6 OBJETIVO GENERAL

Diseño técnico de un laboratorio de redes y seguridad informática en la Universidad Minuto de Dios Centro Regional Soacha, para la capacitación en competencias específicas de los diferentes programas técnicos tecnológicos y profesionales que ofrece la institución educativa.

1.1.7 OBJETIVOS ESPECÍFICOS

- Elaborar el diseño lógico de la red del laboratorio y sus políticas de seguridad garantizando su funcionalidad y minimizando los riesgos de vulnerabilidad para la red.
- Evaluar y estructurar el diseño físico del laboratorio en su distribución en el espacio, en la selección de los dispositivos necesarios tanto de hardware como de software, garantizando un adecuado manejo de este y unas prácticas eficientes en el.
- Realizar el análisis de requisitos según las normas ANSI/EIA/TIA 568-A y 568-B para asegurar el perfecto funcionamiento del laboratorio de Redes y Seguridad Informática en el salón 311 de la Universidad Minuto de Dios Centro regional Soacha.
- Establecer los lineamientos de uso del laboratorio según el plan de estudios de la carrera de redes y seguridad informática, obteniendo la posibilidad de realizar en él la totalidad de las prácticas que se puedan generar en el transcurso de la carrera.

1.1.8 JUSTIFICACION

La Corporación Universitaria Minuto de Dios - Regional Soacha, tiene la necesidad de implementar un laboratorio para las prácticas de los estudiantes de los programas de Ingeniería de Sistemas Tecnología en Redes y Seguridad Informática, , que cuente con equipos de prueba y herramientas, que garanticen la infraestructura apropiada que demanda un proceso de mediación pedagógica y facilite de esta manera el proceso de aprendizaje e interiorización de las competencias específicas de cada uno de los programas que realizan sus prácticas allí, según el modelo de aprendizaje que imparte la universidad y su visión " la formación en Educación para el Desarrollo; la alta calidad de sus programas académicos estructurados por ciclos y competencias; su impacto en la cobertura originado en el número de sus Sedes y la gran facilidad de acceso a sus programas", es de gran importancia para sus estudiantes tener en su proceso un lugar en donde los conocimientos adquiridos en su formación sean llevados a la practica y así tener un mayor desenvolvimiento en su futuro personal y laboral que en si es lo que se busca al ingresar a una universidad y tomar parte del aprendizaje que allí se imparte a la comunidad, ya que a nivel profesional la parte práctica es lo más importante para así dar a conocer la metodología que tiene incorporada la universidad. Dándola a conocer permitiendo con esto aumentar el nombre y prestigio de está beneficiando todo egresado con miras al campo laboral ya que va a ser más factible su recibimiento en cualquier organización por la calidad en auge de su universidad.

Con lo anterior como respuesta a esta necesidad damos a conocer el análisis y diseño técnico de un laboratorio de redes y así expresar nuestra preocupación por la falta de uno en este proceso de obtención de conocimiento y dejar un lineamiento para posiblemente una solución por parte de la universidad.

1.1.9 HIPOTESIS GENERAL

La falta de un sitio optimo y especializado para las practicas en la carrera tecnológica de redes y seguridad informática esta bajando el nivel de conocimiento con que los estudiantes de la Corporación Universitaria Minuto de Dios, Regional Soacha están culminando sus estudios, lo que representa la ausencia de un diseño técnico de un laboratorio como inicio para comenzar a suplir la necesidad que vive la universidad.

1.1.10 HIPOTESIS DE TRABAJO

El diseño técnico de un laboratorio de redes es el punto de inicio para su implementación y así solventar las necesidades de la carrera tecnológica de Redes y seguridad informática en la Corporación Universitaria Minuto de Dios, Regional Soacha.

1.1.11 MISION

A través del diseño técnico del laboratorio de redes abrir puertas para la pronta elaboración de este por parte de la Corporación Universitaria Minuto de Dios, Regional Soacha mejorando la calidad del talento humano de sus egresados en Redes y Seguridad Informática, por la modernidad de su infraestructura y equipos de laboratorio.

1.1.12 VISION

Como visión para el 2015 la Corporación Universitaria Minuto de Dios centro regional Soacha debe contar en sus instalaciones con un laboratorio de Redes y Seguridad Informática optimo, que permita a los estudiantes del programa de Tecnología en Redes y Seguridad Informática, desarrollar competencias propias de su quehacer laboral, a través de prácticas acompañadas o en actividades de tiempo independiente, que evidencien las habilidades y competencias del egresado de la Universidad.

1.1.13 ANTECEDENTES

La universidad Minuto de Dios regional Soacha, cuenta en sus instalaciones con 11 salas de informática, 2 de electrónica, 1 de diseño. Las cuales tienen una administración guiada hacia el uso de todas las carreras en general y algunas especializadas en informática.

Estas salas trabajan bajo el sistema operativo xp, con dos tipos de usuarios; el administrador que es la persona encargada de dar soporte y de la configuración

de estos equipos, y estudiantes que son cualquier persona vinculada a la universidad en formación académica la cual puede hacer uso de estos. Los equipos de estas salas manejan software licenciado 2003 como es el caso de office y el sistema operativo ya mencionado xp, manejan programas como java mysql visual Basic c++ (aclarando su uso para programación y gestión de bases de datos), packet tracer (gestión y administración de redes simuladas), CorelDraw (Diseño y dibujo), Helisa, Siigo (Contabilidad) Cuentan con un canal ADSL y una interconexión entre ellas a través de la red por switches y puntos de acceso inalámbrico, además de comunicación con la sede de la 80 siendo controladas por su proxy de red, no permiten cambios a nivel de hardware ni de software y tienen un funcionamiento estándar guiado siempre a lo ya establecido.

1.1.14 MARCO HISTORICO

Cada uno de los tres últimos siglos fue dominado por una tecnología. El siglo XVIII fue la era de los grandes sistemas mecánicos que acompañaron la Revolución Industrial. El siglo XIX fue la edad de la máquina de vapor. Durante el siglo XX la tecnología clave fue la obtención, el procesamiento y la distribución de la información. Entre otros acontecimientos, vimos la instalación de redes mundiales de telefonía, la invención de la radio y la televisión, el nacimiento y crecimiento sin precedentes de la industria de la computación, así como el lanzamiento de satélites de comunicaciones.

Como resultado del rápido progreso tecnológico, estas áreas están convergiendo de una manera acelerada y las diferencias entre la recolección, transportación, almacenamiento y procesamiento de la información están desapareciendo rápidamente. Organizaciones con cientos de oficinas dispersas en una amplia área geográfica esperan de manera rutinaria poder examinar el estado actual incluso de su sucursal más distante con sólo oprimir un botón. Al aumentar nuestra capacidad de obtener, procesar y distribuir información, la demanda de procesamiento de información cada vez más complejo crece incluso con más celeridad.

Aunque la industria de la computación aún es joven en comparación con otras industrias (como la automotriz y la aeronáutica), ha progresado espectacularmente en poco tiempo. Durante las dos primeras décadas de su existencia, los sistemas de computación estaban altamente centralizados, por lo general, en una sala grande e independiente. Con frecuencia, estas salas tenían paredes de cristal a través de las cuales los visitantes podían atisbar la maravilla electrónica que encerraban. Las compañías o universidades medianas apenas llegaban a tener

una o dos computadoras, en tanto que las instituciones grandes tenían, cuando mucho, una docena. La idea de que en veinte años se pudieran producir en masa millones de computadoras igualmente poderosas pero más pequeñas que un timbre postal era ciencia-ficción.

La fusión de las computadoras y las comunicaciones ha tenido una influencia profunda en la manera en que están organizados los sistemas computacionales. Actualmente, el concepto de “centro de cómputo” como un espacio amplio con una computadora grande a la que los usuarios llevaban su trabajo a procesar es totalmente obsoleto. El modelo antiguo de una sola computadora que realiza todas las tareas computacionales de una empresa ha sido reemplazado por otro en el que un gran número de computadoras separadas pero interconectadas hacen el trabajo. Estos sistemas se denominan redes de computadoras. El diseño y la organización de estas redes es el objetivo de este Proyecto.

Se dice que dos computadoras están interconectadas si pueden intercambiar información. No es necesario que la conexión se realice mediante un cable de cobre; también se pueden utilizar las fibras ópticas, las microondas, los rayos infrarrojos y los satélites de comunicaciones. Las redes tienen varios tamaños, formas y figuras, como veremos más adelante. Aunque a algunas personas les parezca extraño, ni Internet ni Web son una red de computadoras. La respuesta rápida es: Internet no es una red única, sino una red de redes, y Web es un sistema distribuido que se ejecuta sobre Internet.

Existe una gran confusión entre una red de computadoras y un sistema distribuido. La diferencia principal radica en que, en un sistema distribuido, un conjunto de computadoras independientes aparece ante sus usuarios como un sistema consistente y único. Por lo general, tiene un modelo o paradigma único que se presenta a los usuarios. Con frecuencia, una capa de software que se ejecuta sobre el sistema operativo, denominada middleware, es la responsable de implementar este modelo. Un ejemplo bien conocido de un sistema distribuido es World Wide Web, en la cual todo se ve como un documento (una página Web). En una red de computadoras no existe esta consistencia, modelo ni software. Los usuarios están expuestos a las máquinas reales, y el sistema no hace ningún intento porque las máquinas se vean y actúen de manera similar. Si las máquinas tienen hardware diferente y distintos sistemas operativos, eso es completamente transparente para los usuarios. Si un usuario desea ejecutar un programa de una máquina remota, debe registrarse en ella y ejecutarlo desde ahí. De hecho, un sistema distribuido es un sistema de software construido sobre una red. El software le da un alto grado de consistencia y transparencia. De este modo, la diferencia entre una red y un sistema distribuido está en el software (sobre todo en el sistema operativo), más que en el hardware.

No obstante, tienen muchas cosas en común. Por ejemplo, tanto los sistemas distribuidos como las redes de computadoras necesitan mover archivos. La diferencia está en quién invoca el movimiento, el sistema o el usuario. Aunque el objetivo principal de este libro son las redes, muchos de los temas se relacionan con los sistemas distribuidos

1.1.15 MARCO LEGAL

Normas y estándares Redes y cableado estructurado

ANSI/TIA/EIA 569-A Commercial Building Standard for Telecommunications Pathways and Spaces. (Febrero 1998)

ANSI/TIA/EIA 569-A-1 Addendum 1 Surface Raceways. (Abril 2000)

ANSI/TIA/EIA 569-A-2 Addendum 2 Furniture Pathways and Spaces. (Abril 2000)

ANSI/TIA/EIA 569-A-3 Addendum 3 Access Floors. (Marzo 2000)

ANSI/TIA/EIA 569-A-4 Addendum 4 Poke-Thru Fittings. (Marzo 2000)

ANSI/TIA/EIA 569-A-5 Addendum 5 Under floor Pathway.

ANSI/TIA/EIA 569-A-6 Addendum 6 Multitenant Pathways and Spaces (Setiembre 2001).

ANSI/TIA/EIA 569-A-7 Addendum 7 Cable Trays and Wire ways (Diciembre 2001).

ANSI/TIA/EIA-569 (CSA T530) Commercial Building Standards for Telecommunications Pathways and Spaces.

ANSI/TIA/EIA-607 (CSA T527) Grounding and Bonding Requirements for Telecommunications in Commercial Buildings.

ANSI/J-STD-607-A-2002

ANSI/TIA/EIA-568-A (CSA T529-95 Commercial Building Telecommunications Cabling Standard. (Octubre 1995)

ANSI/TIA/EIA 568-A-1 Propagation Delay and Delay Skew Specifications for 100 ohm 4-pair Cable. (Setiembre 1997)

ANSI/TIA/EIA 568-A-2 Corrections and Additions to TIA/EIA-568-A. (Agosto 1998)

ANSI/TIA/EIA 568-A-3 Hybrid Cables. (Diciembre 1998)

ANSI/TIA/EIA 568-A-4 Production Modular Cord NEXT Loss Test Method and Requirements for UTP Cabling. (Diciembre 1999)

ANSI/TIA/EIA 568-A-5 Transmission Performance Specifications for 4-pair 100 ohm Category 5e Cabling. (Enero 2000)

ANSI/TIA/EIA-568-B (CSA T529-95 Commercial Building Telecommunications Cabling Standard.

ANSI/TIA/EIA 568-B.1 Commercial Building Telecommunications Cabling Standard, Part 1: General Requirements. (Abril 2001)

ANSI/TIA/EIA 568-B.1-1 Telecommunications Cabling Standard, Part 1: General Requirements - Addendum 1 - Minimum 4-Pair UTP and 4-Pair ScTP Patch Cable Bend Radius (Mayo 2001)

ANSI/TIA/EIA 568-B.2 Commercial Building Telecommunications Cabling Standard - Part 2: Balanced Twisted Pair Cabling Components (Mayo 2001)

ANSI/TIA/EIA 568-B.2-1 Commercial Building Telecommunications Cabling Standard, Part 2 Addendum 1 - Transmission Performance Specifications for 4-Pair 100 Ohm Category 6 Cabling (Junio 2002)

ANSI/TIA/EIA 568-B.2-2 Commercial Building Telecommunications Cabling Standard - Part 2: Balanced Twisted-Pair Cabling Components - Addendum 2 (Diciembre 2001)

ANSI/TIA/EIA 568-B.2-3 Commercial Building Telecommunications Cabling Standard - Part 2: Balanced Twisted-Pair Cabling - Addendum 3 – Additional Considerations for Insertion Loss and Return Loss Pass/Fail Determination (Marzo 2002)

ANSI/TIA/EIA 568-B.2-4 Commercial Building Telecommunications Cabling Standard - Part 2: Balanced Twisted Pair Components - Addendum 4 - Solderless Connection Reliability Requirements for Copper Connecting Hardware (Junio 2002)

ANSI/TIA/EIA 568-B.3 Optical Fiber Cabling Components. (Abril 2000)

ANSI/TIA/EIA 568-B.3-1 Optical Fiber Cabling Components Standard - Addendum 1 - Additional Transmission Performance Specifications for 50/125 um Optical Fiber Cables (Abril 2002)

1.1.16 MARCO TEÓRICO

Para el análisis técnico del diseño del laboratorio de redes y seguridad informática, es de suma importancia los siguientes temas para profundizar sobre el proceso llevado a cabo:

El modelo de referencia OSI

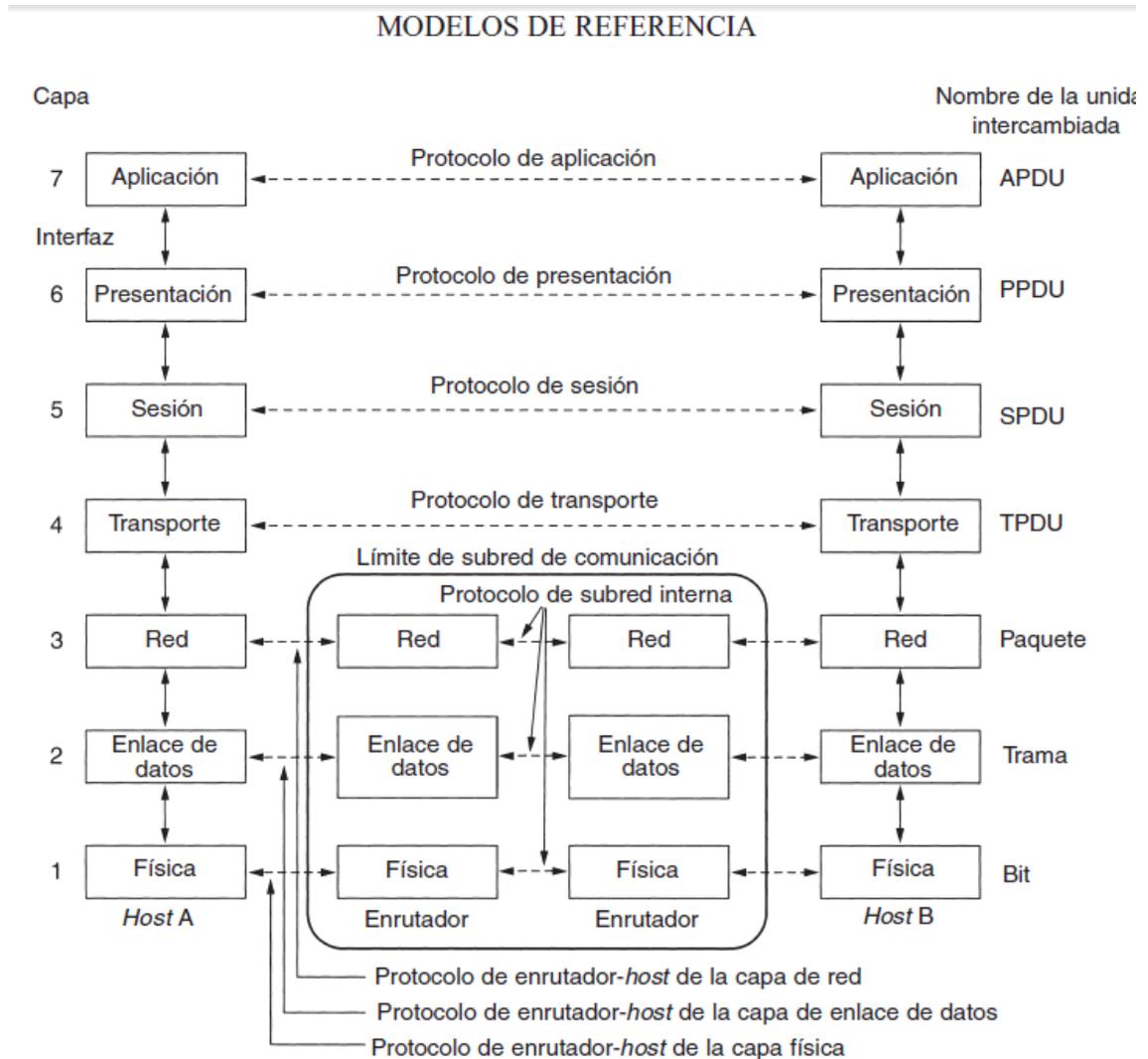


FIGURA 1 MODELOS DE REFERENCIA OSI

El modelo OSI está basado en una propuesta desarrollada por la ISO (Organización Internacional de Estándares) como un primer paso hacia la estandarización internacional de los protocolos utilizados en varias capas (Day y Zimmermann, 1983). Fue revisado en 1995 (Day, 1995). El modelo se llama OSI (Interconexión de Sistemas Abiertos) de ISO porque tiene que ver con la conexión de sistemas abiertos, es decir, sistemas que están abiertos a la comunicación con otros sistemas. Para abreviar, lo llamaremos modelo OSI.

El modelo OSI tiene siete capas. Podemos resumir brevemente los principios que se aplicaron para llegar a dichas capas:

1. Una capa se debe crear donde se necesite una abstracción diferente.
2. Cada capa debe realizar una función bien definida.
3. La función de cada capa se debe elegir con la intención de definir protocolos estandarizados internacionalmente.
4. Los límites de las capas se deben elegir a fin de minimizar el flujo de información a través de las interfaces.
5. La cantidad de capas debe ser suficientemente grande para no tener que agrupar funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se vuelva inmanejable. A continuación analizaremos una por una cada capa del modelo, comenzando con la capa inferior. Observe que el modelo OSI no es en sí una arquitectura de red, debido a que no especifica los servicios y protocolos exactos que se utilizarán en cada capa. Sólo indica lo que debe hacer cada capa. Sin embargo, ISO también ha producido estándares para todas las capas, aunque éstos no son parte del modelo de referencia mismo. Cada uno se ha publicado como un estándar internacional separado.

La capa física

En esta capa se lleva a cabo la transmisión de bits puros a través de un canal de comunicación. Los aspectos del diseño implican asegurarse de que cuando un lado envía un bit 1, éste se reciba en el otro lado como tal, no como bit 0. Las preguntas típicas aquí son: ¿cuántos voltios se deben emplear para representar un 1 y cuántos para representar un 0?, ¿cuántos nanosegundos dura un bit?, ¿la transmisión se debe llevar a cabo en ambas direcciones al mismo tiempo?, ¿cómo

se establece la conexión inicial y cómo se finaliza cuando ambos lados terminan?, ¿cuántos pines tiene un conector de red y para qué se utiliza cada uno? Los aspectos de diseño tienen que ver mucho con interfaces mecánicas, eléctricas y de temporización, además del medio físico de transmisión, que está bajo la capa física.

La capa de enlace de datos

La tarea principal de esta capa es transformar un medio de transmisión puro en una línea de comunicación que, al llegar a la capa de red, aparezca libre de errores de transmisión. Logra esta tarea haciendo que el emisor fragmente los datos de entrada en tramas de datos (típicamente, de algunos cientos o miles de bytes) y transmitiendo las tramas de manera secuencial. Si el servicio es confiable, el receptor confirma la recepción correcta de cada trama devolviendo una trama de confirmación de recepción. Otra cuestión que surge en la capa de enlace de datos (y en la mayoría de las capas superiores) es cómo hacer que un transmisor rápido no sature de datos a un receptor lento. Por lo general se necesita un mecanismo de regulación de tráfico que indique al transmisor cuánto espacio de búfer tiene el receptor en ese momento. Con frecuencia, esta regulación de flujo y el manejo de errores están integrados.

Las redes de difusión tienen un aspecto adicional en la capa de enlace de datos: cómo controlar el acceso al canal compartido. Una subcapa especial de la capa de enlace de datos, la subcapa de control de acceso al medio, se encarga de este problema.*

La capa de red

Esta capa controla las operaciones de la subred. Un aspecto clave del diseño es determinar cómo se enrutan los paquetes desde su origen a su destino. Las rutas pueden estar basadas en tablas estáticas (enrutamiento estático) codificadas en la red y que rara vez cambian.

Capa de Aplicación

Capa Nombre de la unidad intercambiada Protocolo de aplicación Protocolo de presentación Límite de subred de comunicación Protocolo de subred interna Protocolo de transporte Protocolo de sesión Protocolo de enrutador-host de la

capa de red Protocolo de enrutador-host de la capa física Protocolo de enrutador-host de la capa de enlace de datos Sesión Transporte Red Enlace de datos Enlace de datos Física Enrutador Red Enlace de datos Física Host A Enrutador Presentación Aplicación Sesión Transporte Red Enlace de datos Física Presentación Paquete PDU APDU SPDU TPDU Trama Bit Host B Interfaz *En esta capa se define el direccionamiento físico, que permite a los hosts identificar las tramas destinadas a ellos. Este direccionamiento es único, identifica el hardware de red que se está usando y el fabricante, y no se puede cambiar. (N. del R.T.) **En el enrutamiento estático la ruta que seguirán los paquetes hacia un destino particular es determinada por el administrador de la red. Las rutas también pueden determinarse cuando los enrutadores intercambian información de enrutamiento (enrutamiento dinámico). En este tipo de enrutamiento los enrutadores deciden la ruta que seguirán los paquetes hacia un destino sin la intervención del administrador de red. En el enrutamiento dinámico las rutas pueden cambiar para reflejar la topología o el estado de la red. (N. del R.T.) Si hay demasiados paquetes en la subred al mismo tiempo, se interpondrán en el camino unos y otros, lo que provocará que se formen cuellos de botella. La responsabilidad de controlar esta congestión también pertenece a la capa de red, aunque esta responsabilidad también puede ser compartida por la capa de transmisión. De manera más general, la calidad del servicio proporcionado (retardo, tiempo de tránsito, inestabilidad, etcétera) también corresponde a la capa de red. Cuando un paquete tiene que viajar de una red a otra para llegar a su destino, pueden surgir muchos problemas. El direccionamiento utilizado por la segunda red podría ser diferente del de la primera.* La segunda podría no aceptar todo el paquete porque es demasiado largo. Los protocolos podrían ser diferentes, etcétera. La capa de red tiene que resolver todos estos problemas para que las redes heterogéneas se interconecten.

En las redes de difusión, el problema de enrutamiento es simple, por lo que la capa de red a veces es delgada o, en ocasiones, ni siquiera existe.

La capa de transporte

La función básica de esta capa es aceptar los datos provenientes de las capas superiores, dividirlos en unidades más pequeñas si es necesario, pasar éstas a la capa de red y asegurarse de que todas las piezas lleguen correctamente al otro extremo. Además, todo esto se debe hacer con eficiencia y de manera que aisle a las capas superiores de los cambios inevitables en la tecnología del hardware. La capa de transporte también determina qué tipo de servicio proporcionar a la capa de sesión y, finalmente, a los usuarios de la red. El tipo de conexión de transporte más popular es un canal punto a punto libre de errores que entrega mensajes o bytes en el orden en que se enviaron. Sin embargo, otros tipos de servicio de

transporte posibles son la transportación de mensajes aislados, que no garantiza el orden de entrega, y la difusión de mensajes a múltiples destinos. El tipo de servicio se determina cuando se establece la conexión. (Como observación, es imposible alcanzar un canal libre de errores; lo que se quiere dar a entender con este término es que la tasa de error es tan baja que se puede ignorar en la práctica.) La capa de transporte es una verdadera conexión de extremo a extremo, en toda la ruta desde el origen hasta el destino. En otras palabras, un programa en la máquina de origen lleva a cabo una conversación con un programa similar en la máquina de destino, usando los encabezados de mensaje y los mensajes de control. En las capas inferiores, los protocolos operan entre cada máquina y sus vecinos inmediatos, y no entre las máquinas de los extremos, la de origen y la de destino, las cuales podrían estar separadas por muchos enrutadores.

La capa de sesión

Esta capa permite que los usuarios de máquinas diferentes establezcan sesiones entre ellos. Las sesiones ofrecen varios servicios, como el control de diálogo (dar seguimiento de a quién le toca *El direccionamiento usado en esta capa es un direccionamiento lógico, diferente al direccionamiento físico empleado en la capa de enlace de datos. Este direccionamiento lógico permite que una interfaz o puerto pueda tener más de una dirección de capa de red. (N. del R.T.) Transmitir), administración de token (que impide que las dos partes traten de realizar la misma operación crítica al mismo tiempo) y sincronización (la adición de puntos de referencia a transmisiones largas para permitirles continuar desde donde se encontraban después de una caída).

La capa de presentación

A diferencia de las capas inferiores, a las que les corresponde principalmente mover bits, a la capa de presentación le corresponde la sintaxis y la semántica de la información transmitida. A fin de que las computadoras con diferentes representaciones de datos se puedan comunicar, las estructuras de datos que se intercambiarán se pueden definir de una manera abstracta, junto con una codificación estándar para su uso "en el cable". La capa de presentación maneja estas estructuras de datos abstractas y permite definir e intercambiar estructuras de datos de un nivel más alto (por ejemplo, registros bancarios).

La capa de aplicación

Esta capa contiene varios protocolos que los usuarios requieren con frecuencia. Un protocolo de aplicación de amplio uso es HTTP (Protocolo de Transferencia de Hipertexto), que es la base de World Wide Web. Cuando un navegador desea una página Web, utiliza este protocolo para enviar al servidor el nombre de dicha página. A continuación, el servidor devuelve la página. Otros protocolos de aplicación se utilizan para la transferencia de archivos, correo electrónico y noticias en la red.

El modelo de referencia TCP/IP

Tratemos ahora el modelo de referencia usado en la abuela de todas las redes de computadoras de área amplia, ARPANET, y en su sucesora, la Internet mundial. Aunque daremos más adelante una breve historia de ARPANET, es útil mencionar algunos de sus aspectos ahora. ARPANET fue una red de investigación respaldada por el DoD (Departamento de Defensa de Estados Unidos). Con el tiempo, conectó cientos de universidades e instalaciones gubernamentales mediante líneas telefónicas alquiladas. Posteriormente, cuando se agregaron redes satelitales y de radio, los protocolos existentes tuvieron problemas para interactuar con ellas, por lo que se necesitaba una nueva arquitectura de referencia. De este modo, la capacidad para conectar múltiples redes en una manera sólida fue una de las principales metas de diseño desde sus inicios. Más tarde, esta arquitectura se llegó a conocer como el modelo de referencia TCP/IP, de acuerdo con sus dos protocolos primarios. Su primera definición fue en (Cerf y Kahn, 1974). Posteriormente se definió en (Leiner y cols., 1985). La filosofía del diseño que respalda al modelo se explica en (Clark, 1988). Ante el temor del DoD de que algunos de sus valiosos hosts, enrutadores y puertas de enlace de inter redes explotaran en un instante, otro objetivo fue que la red pudiera sobrevivir a la pérdida de hardware de la subred, sin que las conversaciones existentes se interrumpieran. En otras palabras, el DoD quería que las conexiones se mantuvieran intactas en tanto las máquinas de origen y destino estuvieran funcionando, aunque algunas de las máquinas o líneas de transmisión intermedias quedaran fuera de operación repentinamente. Además, se necesitaba una arquitectura flexible debido a que se preveían aplicaciones con requerimientos divergentes, desde transferencia de archivos a transmisión de palabras en tiempo real.

La capa de Interred.

Todos estos requerimientos condujeron a la elección de una red de conmutación de paquetes basada en una capa de inter red no orientada a la conexión. Esta capa, llamada capa de inter red, es la pieza clave que mantiene unida a la arquitectura. Su trabajo es permitir que los hosts inyecten paquetes dentro de cualquier red y que éstos viajen a su destino de manera independiente (podría ser en una red diferente). Tal vez lleguen en un orden diferente al que fueron enviados, en cuyo caso las capas más altas deberán ordenarlos, si se desea una entrega ordenada. Observe que aquí el concepto “inter red” se utiliza en un sentido genérico, aun cuando esta capa se presente en Internet. Aquí la analogía es con el sistema de correo tradicional. Una persona puede depositar una secuencia de cartas internacionales en un buzón y, con un poco de suerte, la mayoría de ellas se entregará en la dirección correcta del país de destino. Es probable que durante el trayecto, las cartas viajen a través de una o más puertas de enlace de correo internacional, pero esto es transparente para los usuarios. Además, para los usuarios también es transparente el hecho de que cada país (es decir, cada red) tiene sus propios timbres postales, tamaños preferidos de sobre y reglas de entrega.

La capa de inter red define un paquete de formato y protocolo oficial llamado IP (Protocolo de Internet). El trabajo de la capa de inter red es entregar paquetes IP al destinatario. Aquí, el enrutamiento de paquetes es claramente el aspecto principal, con el propósito de evitar la congestión. Por estas razones es razonable decir que la capa de inter red del modelo TCP/IP es similar en funcionalidad a la capa de red del modelo OSI.

MODELOS DE REFERENCIA

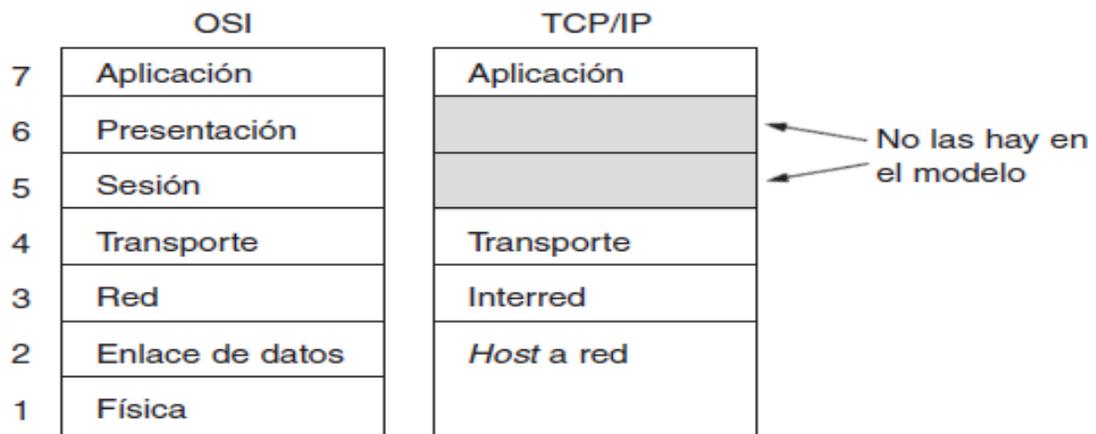


FIGURA 2 MODELOS DE REFERENCIA

La capa de transporte

La capa que está arriba de la capa de inter red en el modelo TCP/IP se llama capa de transporte. Está diseñada para permitir que las entidades iguales en los hosts de origen y destino puedan llevar a cabo una conversación, tal como lo hace la capa de transporte OSI. Aquí se han definido dos protocolos de transporte de extremo a extremo. El primero, TCP (Protocolo de Control de Transmisión), es un protocolo confiable, orientado a la conexión, que permite que un flujo de bytes que se origina en una máquina se entregue sin errores en cualquier otra máquina en la Inter red .Divide el flujo de bytes entrantes en mensajes discretos y pasa cada uno de ellos a la capa de inter red. En el destino, el proceso TCP receptor re ensambla en el flujo de salida los mensajes recibidos. TCP también maneja el control de flujo para asegurarse de que un emisor rápido no sature a un receptor lento con más mensajes de los que puede manejar.

El segundo protocolo de esta capa, UDP (Protocolo de Datagrama de Usuario), es un protocolo no confiable y no orientado a la conexión para aplicaciones que no desean la secuenciación o el control de flujo de TCP y que desean proporcionar el suyo. También tiene un amplio uso en consultas únicas de solicitud-respuesta de tipo cliente-servidor en un solo envío, así como aplicaciones en las que la entrega puntual es más importante que la precisa, como en la transmisión de voz o vídeo. Puesto que el modelo se desarrolló, se ha implementado IP en muchas otras redes.

La capa de aplicación

El modelo TCP/IP no tiene capas de sesión ni de presentación. No se han necesitado, por lo que no se incluyen. La experiencia con el modelo OSI ha probado que este punto de vista es correcto:

Son de poco uso para la mayoría de las aplicaciones. Aplicación Presentación Sesión Transporte Red Enlace de datos Física Aplicación Transporte Inter red Host a red 7 6 5 4 3 2 1 OSI TCP/IP No las hay en el modelo

Arriba de la capa de transporte está la capa de aplicación. Contiene todos los protocolos de nivel más alto. Los primeros incluyeron una terminal virtual (TELNET), transferencia de archivos (FTP) y correo electrónico (SMTP), como se muestra en la figura 1-22. El protocolo de terminal virtual permite que un usuario en una máquina se registre en una máquina remota y trabaje ahí. El protocolo de

transferencia de archivos proporciona una manera de mover con eficiencia datos de una máquina a otra. El correo electrónico era originalmente sólo un tipo de transferencia de archivos, pero más tarde se desarrolló un protocolo especializado (SMTP) para él. Con el tiempo, se han agregado muchos otros protocolos: DNS (Sistema de Nombres de Dominio) para la resolución de nombres de host en sus direcciones de red; NNTP, para transportar los artículos de noticias de USENET; HTTP, para las páginas de Word Wide Web, y muchos otros.

La capa host a red

Debajo de la capa de inter red hay un gran vacío. El modelo de referencia TCP/IP en realidad no dice mucho acerca de lo que pasa aquí, excepto que puntualiza que el host se tiene que conectar a la red mediante el mismo protocolo para que le puedan enviar paquetes IP. Este protocolo no está definido y varía de un host a otro y de una red a otra. Este tema rara vez se trata en libros y artículos sobre TCP/IP.

Cableado estructurado

Este estándar tiene en cuenta tres conceptos fundamentales relacionados con telecomunicaciones y edificios:

1. Los edificios son dinámicos. Durante la existencia de un edificio, las remodelaciones son comunes, y deben ser tenidas en cuentas desde el momento del diseño. Este estándar reconoce que el cambio ocurre y lo tienen en cuenta en sus recomendaciones para el diseño de las canalizaciones de telecomunicaciones.
2. Los sistemas de telecomunicaciones son dinámicos. Durante la existencia de un edificio, las tecnologías y los equipos de telecomunicaciones pueden cambiar dramáticamente. Este estándar reconoce este hecho siendo tan independiente como sea posible de proveedores y tecnologías de equipo.
3. Telecomunicaciones es más que “voz y datos”. El concepto de Telecomunicaciones también incorpora otros sistemas tales como control ambiental, seguridad, audio, televisión, alarmas y sonido. De hecho, telecomunicaciones incorpora todos los sistemas de “bajo voltaje” que transportan información en los edificios.

El estándar identifica seis componentes en la infraestructura edilicia:

- Instalaciones de Entrada
- Sala de Equipos
- Canalizaciones de “Montantes” (“Back-bone”)
- Armarios de Telecomunicaciones
- Canalizaciones horizontales
- Áreas de trabajo

Ver figura 1 en anexo figuras Backbone.

Instalaciones de Entrada

Se define como el lugar en el que ingresan los servicios de telecomunicaciones al edificio y/o dónde llegan las canalizaciones de interconexión con otros edificios de la misma corporación (por ejemplo, si se trata de un “campus”). Las “instalaciones de entrada” pueden contener dispositivos de interfaz con las redes públicas prestadoras de servicios de telecomunicaciones, y también equipos de telecomunicaciones. Estas interfaces pueden incluir borneras (por ejemplo telefónicas) y equipos activos (por ejemplo módems). El estándar recomienda que la ubicación de las “Instalaciones de entrada” sean un lugar seco, cercanos a las canalizaciones de “montantes” verticales (Back-Bone)

Sala de Equipos

Se define como el espacio dónde se ubican los equipos de telecomunicaciones comunes al edificio. Estos equipos pueden incluir centrales telefónicas (PBX), equipos informáticos (servidores), Centrales de video, etc. Sólo se admiten equipos directamente relacionados con los sistemas de telecomunicaciones. En el diseño y ubicación de la sala de equipos, se deben considerar:

- Posibilidades de expansión. Es recomendable prever el crecimiento en los equipos que irán ubicados en la sala de equipos, y prever la posibilidad de expansión de la sala.
- Evitar ubicar la sala de equipos en lugar dónde puede haber filtraciones de agua, ya sea por el techo o por las paredes

- Facilidades de acceso para equipos de gran tamaño.
- La estimación de espacio para esta sala es de 0.07 m² por cada 10 m² de área utilizable del edificio. (Si no se dispone de mejores datos, se puede estimar el área utilizable como el 75% del área total). En edificios de propósitos específicos, como ser Hoteles y Hospitales, el área utilizable es generalmente mucho más grande que el área efectiva de trabajo. En estos casos, el cálculo puede hacerse en función del área efectiva de trabajo. En todos los casos, el tamaño mínimo recomendado es de 13.5 m² (es decir, una sala de unos 3.7 x 3.7 m).
- Es recomendable que esté ubicada cerca de las canalizaciones “montantes” (backbone), ya que a la sala de equipos llegan generalmente una cantidad considerable de cables desde estas canalizaciones.

Otras consideraciones deben tenerse en cuenta, como por ejemplo:

- Fuentes de interferencia electromagnética
- Vibraciones
- Altura adecuada
- Iluminación
- Consumo eléctrico
- Prevención de incendios
- Aterramientos

Canalizaciones de “Back-Bone”

Se distinguen dos tipos de canalizaciones de “back-bone”: Canalizaciones externas, entre edificios y Canalizaciones internas al edificio.

Canalizaciones externas entre edificios

Las canalizaciones externas entre edificios son necesarias para interconectar “Instalaciones de Entrada” de varios edificios de una misma corporación, en ambientes del tipo “campus”. La recomendación ANSI/TIA/EIA-569 admite, para estos casos, cuatro tipos de canalizaciones: Subterráneas, directamente enterradas, aéreas, y en túneles.

Canalizaciones Subterráneas

Las canalizaciones subterráneas consisten en un sistema de ductos y cámaras de inspección. Los ductos deben tener un diámetro mínimo de 100 mm (4 “). No sea admiten más de dos quiebres de 90 grados.

Canalizaciones directamente enterradas

En estos casos, los cables de telecomunicaciones quedan enterrados. Es importante que los cables dispongan, en estos casos, de la protección es adecuadas (por ejemplo, anti-roedor).

Backbone aéreos

Algunas consideraciones a tener en cuenta al momento de tender cableas aéreas:

- Apariencia del edificio y las áreas circundantes
- Legislación aplicable
- Separación requerida con cableados aéreos eléctricos
- Protecciones mecánicas, carga sobre los puntos de fijación, incluyendo tormentas y vientos

Canalizaciones en túneles

La ubicación de las canalizaciones dentro de túneles deben ser planificadas de manera que permitan el correcto acceso al personal de mantenimiento, y también la separación necesaria con otros servicios.

Canalizaciones internas

Las canalizaciones internas de “backbone”, generalmente llamadas “montantes” son las que vinculan las “instalaciones de entrada” con la “sala de equipos”, y la “sala de equipos” con los “armarios o salas de telecomunicaciones”. Estas canalizaciones pueden ser ductos, bandejas, escalerillas porta cables, etc. Es muy importante que estas canalizaciones tengan los elementos “cortafuegos” de acuerdo a las normas corporativas y/o legales. Las canalizaciones “montantes” pueden ser físicamente verticales u horizontales.

Canalizaciones montantes verticales

Se requieren para unir la sala de equipos con los armarios de telecomunicaciones o las instalaciones de entrada con la sala de equipos en edificios de varios pisos. Generalmente, en edificios de varios pisos, los armarios de telecomunicaciones se encuentran alineados verticalmente, y una canalización vertical pasa por cada piso, desde la sala de equipos. Estas canalizaciones pueden ser realizadas con ductos, bandejas verticales, o escalerillas porta cables verticales. No se admite el uso de los ductos de los ascensores para transportar los cables de telecomunicaciones.

Canalizaciones montantes horizontales

Si los armarios de telecomunicaciones no están alineados verticalmente, son necesarios tramos de “montantes” horizontales. Estas canalizaciones pueden ser realizadas con ductos, bandejas horizontales, o escalerillas porta cables. Pueden ser ubicadas sobre el cielorraso, debajo del piso, o adosadas a las paredes

El estándar TIA-569 admite los siguientes tipos de canalizaciones horizontales:

Ductos bajo piso

En estos casos los ductos son parte de la obra civil. Bajo el piso se puede realizar una “malla” de ductos, disponiendo de líneas determinadas para telecomunicaciones, energía, etc. En las áreas de trabajo se dispone de puntos de acceso a los ductos bajo piso, utilizando “torretas” u otro tipo de accesorios. Como regla general, debe preverse una sección de 650 mm² por cada área de trabajo de 3 puestos que alimente el ducto.

Ductos bajo piso elevado

Los “pisos elevados” consisten en un sistema de soportes sobre el que apoyan lozas generalmente cuadradas. Son generalmente utilizados en salas de equipos. Sin embargo pueden ser también utilizados para oficinas. Debajo de este sistema de soportes puede ser instalado un sistema de ductos para cableado de telecomunicaciones, de energía, etc. No se recomienda tender cables “suelos” debajo del piso elevado.

Las lozas de los pisos elevados deben ser perforadas en los lugares correspondientes a las áreas de trabajo, y sobre éstas perforaciones se deben ubicar “torretas” u otro tipo de accesorios adecuados para la terminación de los cables. Existen varios tipos de estos accesorios, algunos de los cuales quedan arras del piso.

Ductos aparentes

Los ductos aparentes pueden ser metálicos o de PVC, rígidos en ambos casos. No se recomiendan ductos flexibles para las canalizaciones horizontales. Las características de estos ductos y de su instalación deben ser acordes a los requisitos arquitectónicos y edilicios. Se recomienda que no existan tramos mayores a 30 metros sin puntos de registro e inspección, y que no existan más de dos quiebres de 90 grados en cada tramo.

Bandejas

Las bandejas porta cables consisten en estructuras rígidas, metálicas o de PVC, generalmente de sección rectangular (en forma de U). La base y las paredes laterales pueden ser sólidas o caladas. Las bandejas de este tipo pueden o no tener tapa

Las bandejas se instalan generalmente sobre el cielorraso, aunque pueden ser instaladas debajo del cielorraso, o adosadas al paredes.

Ductos sobre cielorraso

Ductos sobre los cielorrasos pueden ser utilizados, siempre y cuando su acceso sea sencillo, por ejemplo, removiendo planchas livianas de cielo raso. Los ductos o bandejas sobre cielorraso deben estar adecuadamente fijados al techo, por medio de colgantes. No se recomienda que estén directamente apoyadas sobre la estructura propia del cielo raso. Los cables sobre cielorraso no pueden estar sueltos, apoyados directamente sobre el cielorraso, sino que deben estar dentro de ductos o bandejas.

Ductos perimetrales

Los ductos perimetrales pueden ser usados para llegar con el cableado horizontal hasta las áreas de trabajo, en caso de oficinas cerradas o tipo “boxes”.

Redes de área local

Las redes de área local (generalmente conocidas como LANs) son redes de propiedad privada que se encuentran en un solo edificio o en un campus de pocos kilómetros de longitud. Se utilizan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de una empresa y de fábricas para compartir recursos (por ejemplo, impresoras) e intercambiar información.

Las LANs son diferentes de otros tipos de redes en tres aspectos: 1) tamaño; 2) tecnología de transmisión, y 3) topología. Las LANs están restringidas por tamaño, es decir, el tiempo de transmisión en el peor de los casos es limitado y conocido de antemano. El hecho de conocer este límite permite utilizar ciertos tipos de diseño, lo cual no sería posible de otra manera. Esto también simplifica la administración de la red. Las LANs podrían utilizar una tecnología de transmisión que consiste en un cable al cual están unidas todas las máquinas, como alguna vez lo estuvo parte de las líneas de las compañías telefónicas en áreas rurales. Las LANs tradicionales se ejecutan a una velocidad de 10 a 100 Mbps, tienen un retardo bajo (microsegundos o nano segundos) y cometen muy pocos errores. Las LANs más nuevas funcionan hasta a 10 Gbps. continuaremos con lo tradicional y mediremos las velocidades de las líneas en megabits por segundo (1 Mbps es

igual a 1, 000,000 de bits por segundo) y gigabits por segundo (1 Gbps es igual a 1,000,000,000 de bits por segundo). Para las LANs de difusión son posibles varias topologías.

Las redes de difusión se pueden dividir aún más en estáticas y dinámicas, dependiendo de cómo se asigne el canal. Una asignación estática típica sería dividir el tiempo en intervalos discretos y utilizar un algoritmo round-robin, permitiendo que cada máquina transmita sólo cuando llegue su turno. La asignación estática desperdicia capacidad de canal cuando una máquina no tiene nada que transmitir al llegar su turno, por lo que la mayoría de los sistemas trata de asignar el canal de forma dinámica (es decir, bajo demanda). Los métodos de asignación dinámica para un canal común pueden ser centralizados o descentralizado.

En el método centralizado hay una sola entidad, por ejemplo, una unidad de arbitraje de bus, la cual determina quién sigue. Esto se podría hacer aceptando solicitudes y tomando decisiones de acuerdo con algunos algoritmos internos. En el método descentralizado de asignación de canal no hay una entidad central; cada máquina debe decidir por sí misma cuándo transmitir. Usted podría pensar que esto siempre conduce al caos, pero no es así.

Redes inalámbricas

La comunicación inalámbrica digital no es una idea nueva. A principios de 1901, el físico italiano Guillermo Marconi demostró un telégrafo inalámbrico desde un barco a tierra utilizando el código Morse (después de todo, los puntos y rayas son binarios). Los sistemas inalámbricos digitales de la actualidad tienen un mejor desempeño, pero la idea básica es la misma. Como primera aproximación, las redes inalámbricas se pueden dividir en tres categorías principales:

1. Interconexión de sistemas.
2. LANs inalámbricas.
3. WANs inalámbricas.

La interconexión de sistemas se refiere a la interconexión de componentes de una computadora que utiliza radio de corto alcance. La mayoría de las computadoras

tiene un monitor, teclado, ratón e impresora, conectados por cables a la unidad central. Son tantos los usuarios nuevos que tienen dificultades para conectar todos los cables en los enchufes correctos (aun cuando suelen estar codificados por colores) que la mayoría de los proveedores de computadoras ofrece la opción de enviar a un técnico a la casa del usuario para que realice esta tarea. En consecuencia, algunas compañías se reunieron para diseñar una red inalámbrica de corto alcance llamada Bluetooth para conectar sin cables estos componentes. Bluetooth también permite conectar cámaras digitales, auriculares, escáneres y otros dispositivos a una computadora con el único requisito de que se encuentren dentro del alcance de la red. Sin cables, sin instalación de controladores, simplemente se colocan, se encienden y funcionan. Para muchas personas, esta facilidad de operación es algo grandioso. En la forma más sencilla, las redes de interconexión de sistemas utilizan el paradigma del maestro y el esclavo. La unidad del sistema es, por lo general, el maestro que trata al ratón, al teclado, etcétera, como a esclavos. El maestro le dice a los esclavos qué direcciones utilizar, cuándo pueden difundir, durante cuánto tiempo pueden transmitir, qué frecuencias pueden utilizar, etcétera.

El siguiente paso en la conectividad inalámbrica son las LANs inalámbricas. Son sistemas en los que cada computadora tiene un módem de radio y una antena mediante los que se puede comunicar con otros sistemas. En ocasiones, en el techo se coloca una antena con la que las máquinas se comunican. Sin embargo, si los sistemas están lo suficientemente cerca, se pueden comunicar de manera directa entre sí en una configuración de igual a igual. Las LANs inalámbricas se están haciendo cada vez más comunes en casas y oficinas pequeñas, donde instalar Ethernet se considera muy problemático, así como en oficinas ubicadas en edificios antiguos, cafeterías de empresas, salas de conferencias y otros lugares. Existe un estándar para las LANs inalámbricas, llamado IEEE 802.11, que la mayoría de los sistemas implementa y que se ha extendido ampliamente.

El tercer tipo de red inalámbrica se utiliza en sistemas de área amplia. La red de radio utilizada para teléfonos celulares es un ejemplo de un sistema inalámbrico de banda ancha baja. Este sistema ha pasado por tres generaciones. La primera era analógica y sólo para voz. La segunda era digital y sólo para voz. La tercera generación es digital y es tanto para voz como para datos. En cierto sentido, las redes inalámbricas celulares son como las LANs inalámbricas, excepto porque las distancias implicadas son mucho más grandes y las tasas de bits son mucho más bajas. Las LANs inalámbricas pueden funcionar a tasas de hasta 50 Mbps en distancias de decenas de metros. Los sistemas celulares funcionan debajo de 1 Mbps, pero la distancia entre la estación base y la computadora o teléfono se mide en kilómetros más que en metros.

Además de estas redes de baja velocidad, también se han desarrollado las redes inalámbricas de área amplia con alto ancho de banda. El enfoque inicial es el acceso inalámbrico a Internet a alta velocidad, desde los hogares y las empresas, dejando a un lado el sistema telefónico. Este servicio se suele llamar servicio de distribución local multipuntos. Lo estudiaremos más adelante. También se ha desarrollado un estándar para éste, llamado IEEE 802.16. La mayoría de las redes inalámbricas se enlaza a la red alámbrica en algún punto para proporcionar acceso a archivos, bases de datos e Internet. Hay muchas maneras de efectuar estas conexiones, dependiendo de las circunstancias.

Muchas personas creen que lo inalámbrico es la onda del futuro (por ejemplo, Bi y cols., 2001; Leeper, 2001; Varshey y Vetter, 2000) pero se ha escuchado una voz disidente. Bob Metcalfe, el inventor de Ethernet, ha escrito: “Las computadoras inalámbricas móviles son como los baños portátiles sin cañería: bacinicas portátiles. Serán muy comunes en los vehículos, en sitios en construcción y conciertos de rock. Mi consejo es que coloque cables en su casa y se quede ahí” (Metcalfe, 1995). La historia podría colocar esta cita en la misma categoría que la explicación de T.J. Watson, presidente de IBM en 1945, de por qué esta empresa no entraba en el negocio de las computadoras: “Cuatro o cinco computadoras deberán ser suficientes para todo el mundo hasta el año 2000”.

Ethernet

Internet y ATM se diseñaron para conectividad de área amplia. Sin embargo, muchas empresas, universidades y otras organizaciones tienen un gran número de computadoras que requieren interconexión. Esta necesidad dio origen a la red de área local. En esta sección diremos algo sobre la LAN más popular: Ethernet. La historia empieza en la prístina Hawaii a principios de la década de 1970. En este caso, “prístina” se puede interpretar como “que no tiene un sistema telefónico funcional”. En tanto los días son más agradables para los vacacionistas cuando no son interrumpidos por el teléfono, no fue así para el investigador Norman Abramson y sus colegas de la Universidad de Hawaii, quienes estuvieron tratando de conectar usuarios de las islas remotas a la computadora principal de Honolulu. Conectar sus propios cables bajo el Océano Pacífico parecía imposible, de modo que buscaron una solución diferente. La primera que encontraron fueron los radios de onda corta. Cada terminal estaba equipada con un radio pequeño de dos frecuencias: un canal ascendente (a la computadora central) y otro descendente (desde la computadora central). Cuando el usuario deseaba conectarse con la computadora, sólo transmitía por el canal ascendente un paquete que contenía los datos. Si en ese instante nadie más estaba transmitiendo, probablemente el paquete saldría y su recepción sería confirmada en el canal descendente. Si había contención por el canal ascendente, la terminal detectaría la falta de confirmación

de recepción y haría otro intento. Puesto que sólo habría un emisor en el canal descendente (la computadora central), nunca habría colisiones ahí. Este sistema, llamado ALOHANET, trabajaba muy bien en condiciones de bajo tráfico pero se caía cuando el flujo de tráfico ascendente era pesado.

En esa misma época, un estudiante llamado Bob Metcalfe hizo su licenciatura en el M.I.T. y luego se mudó para obtener su doctorado en Harvard. Durante sus estudios, conoció el trabajo de Abramson. Se interesó tanto en él que después de graduarse en Harvard decidió pasar el verano en Hawaii trabajando con Abramson antes de empezar a trabajar en el Centro de Investigación de Palo Alto de Xerox (PARC). Cuando llegó al PARC, vio que los investigadores de ahí habían diseñado y construido lo que más tarde se llamarían computadoras personales. Pero las máquinas estaban aisladas. Aplicando su conocimiento del trabajo de Abramson, junto con su colega David Boggs, diseñó e implementó la primera red de área local (Metcalfe y Boggs, 1976).

Llamaron Ethernet al sistema, por lo de luminiferous ether, a través del cual se pensó alguna vez que se propagaba la radiación electromagnética. (Cuando, en el siglo XIX, el físico inglés James Clerk Maxwell descubrió que la radiación electromagnética se podía describir mediante una ecuación de onda, los científicos supusieron que el espacio debía estar lleno de algún medio etéreo en el cual se propagaba la radiación. Sólo después del famoso experimento de Michelson-Morley en 1887, los físicos descubrieron que la radiación electromagnética se podía propagar por el vacío.) Aquí el medio de transmisión no era el vacío, sino un cable coaxial grueso (el éter) de más de 2.5 km de largo (con repetidoras cada 500 metros). El sistema podía contener hasta 256 máquinas por medio de transceptores acoplados al cable. Un cable con múltiples máquinas en paralelo se llama cable de derivación múltiple (multidrop). El sistema se ejecutaba a 2.94 Mbps. En caso de que ya lo hubiera, la computadora se mantenía en espera de que la transmisión actual terminara. Al hacerlo así se evitaba interferir con las transmisiones existentes, dando una mayor eficiencia. ALOHANET no trabajaba de este modo porque para una terminal en una isla era imposible detectar la transmisión de otra terminal en una isla distante. El problema se resolvía con un cable único. A pesar de que la computadora escucha antes de transmitir, surge un problema: ¿qué sucede si dos o más computadoras esperan hasta que se complete la transmisión actual y luego empiezan a transmitir al mismo tiempo? La solución es que cada computadora escuche durante su propia Transmisión y, si detecta interferencia, mande una señal para poner en alerta a todos los transmisores. Después espera un tiempo aleatorio antes de reintentarlo. Si sucede una colisión, el tiempo aleatorio de espera se duplica y así sucesivamente, para separar las transmisiones que están en competencia y dar a alguna la oportunidad de transmitir primero.

La Ethernet de Xerox fue tan exitosa que DEC, Intel y Xerox diseñaron un estándar en 1978 para una Ethernet de 10 Mbps, llamado estándar DIX. Con dos cambios menores, en 1983 el estándar DIX se convirtió en el estándar IEEE 802.3. Por desgracia para Xerox, ya tenía fama de hacer inventos originales (como el de las computadoras personales) y luego fallar en la comercialización de los mismos, como se menciona en un relato titulado *Fumbling the Future* (Smith y Alexander, 1988). Cuando Xerox mostró poco interés en hacer algo con Ethernet aparte de ayudar a estandarizarlo, Metcalfe formó su propia empresa, 3Com, con el propósito de vender adaptadores Ethernet para PCs. Ha vendido más de 100 millones.

Ethernet continuó su desarrollo y aún está en desarrollo. Han salido nuevas versiones a 100 y 1000 Mbps, e incluso más altas. También se ha mejorado el cableado y se han agregado conmutación y otras características. En el capítulo 4 explicaremos Ethernet en detalle. De paso, vale la pena mencionar que Ethernet (IEEE 802.3) no es el único estándar de LAN. El comité también estandarizó Token Bus (802.4) y Token Ring (802.5). La necesidad de tres estándares más o menos incompatibles tiene poco que ver con la tecnología y mucho con la política. En el momento de la estandarización, General Motors estaba impulsando una LAN en la que la topología era la misma que la usada en Ethernet (un cable lineal), pero las computadoras transmitían por turnos pasando un pequeño paquete de computadora a computadora, llamado token. Una computadora podía transmitir sólo si poseía el token, lo que evitaba colisiones. General Motors anunció que este esquema era esencial para la manufactura de automóviles y que no estaba preparado para cambiar su postura. No obstante este anuncio, el 802.4 prácticamente desapareció.

Del mismo modo, IBM tenía su favorito: su Token Ring patentado. En este esquema el token se pasaba a través del anillo y la computadora que poseyera el token podía transmitir antes de poner el token de nuevo en el anillo. A diferencia del 802.4, este esquema, estandarizado como 802.5.

REDES DE EJEMPLO

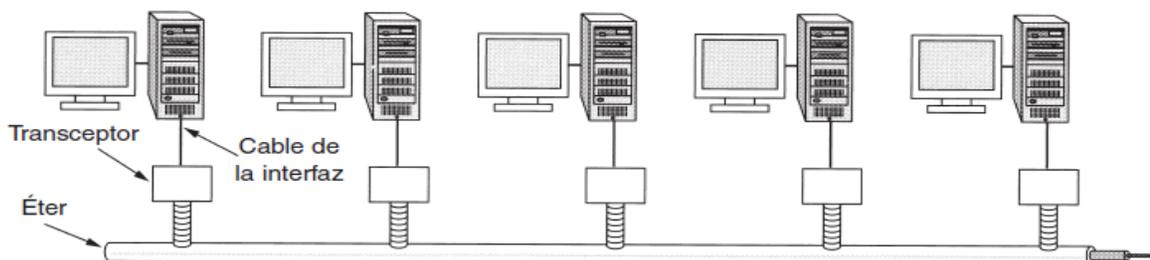


FIGURA 3 ARQUITECTURA DE LA ETHERNET ORIGINAL

Aún se usa en algunos sitios de IBM, pero prácticamente en ninguna parte más. Sin embargo, se está desarrollando una versión de 1 gigabit (802.5v), pero parece poco probable que alcance a Ethernet. Resumiendo, había una guerra entre Ethernet, Token Bus y Token Ring, pero Ethernet ganó, en gran medida porque fue la primera y los retadores no pudieron superarlo. 1.5.4 LANs inalámbricas: 802.11 Casi al mismo tiempo que aparecieron las computadoras portátiles, muchas personas tuvieron el sueño de andar por la oficina y poder conectar a Internet su computadora. En consecuencia, varios grupos empezaron a trabajar para cumplir con esta meta. El método más práctico es equipar las computadoras de la oficina y las portátiles con transmisores y receptores de radio de onda corta que les permitan comunicarse. Este trabajo condujo rápidamente a que varias empresas empezaran a comercializar las LANs inalámbricas.

El problema es que no había compatibilidad entre ninguna de ellas. Esta proliferación de estándares implicaba que una computadora equipada con un radio de marca X no funcionara en un cuarto equipado con una estación de base marca Y. Finalmente, la industria decidió que un estándar de LAN inalámbrica sería una buena idea, por lo que al comité del IEEE que estandarizó las LANs alámbricas se le encargó la tarea de diseñar un estándar para LANs inalámbricas. El estándar resultante se llamó 802.11. En la jerga común se le conoce como WiFi. Es un estándar importante y merece respeto, así que lo llamaremos por su nombre propio, 802.11.

El estándar propuesto tenía que trabajar en dos modos:

1. En presencia de una estación base.
2. En ausencia de una estación base.

En el primer caso, toda la comunicación se hacía a través de la estación base, que en la terminología del 802.11 se conoce como punto de acceso. En el segundo caso, las computadoras podrían enviarse mensajes entre sí directamente. Este modo se llama a veces red ad hoc. Un ejemplo típico es el de dos o más personas que se encuentran juntas en un cuarto no equipado con una LAN inalámbrica y cuyas computadoras se comunican entre sí de manera directa.

La primera decisión fue la más sencilla: cómo llamarlo. Todos los otros estándares LAN tenían números como 802.1, 802.2, hasta 802.10, por lo que el estándar LAN se llamó o publicó como 802.11. El resto fue más difícil.

En particular, varios de los diversos retos que había que enfrentar eran: encontrar una banda de frecuencia adecuada, de preferencia mundial; enfrentar el hecho de que las señales de radio tienen un rango finito; asegurarse de que se mantuviera la privacidad de los usuarios; tomar en cuenta la vida limitada de las baterías; preocuparse por la seguridad humana (¿las ondas de radio causan cáncer?); comprender las implicaciones de la movilidad de las computadoras y, por último, construir un sistema con suficiente ancho de banda para que sea económicamente viable.

Cuando empezó el proceso de estandarización (a mediados de la década de 1990), Ethernet ya había llegado a dominar las redes de área local, por lo que el comité decidió hacer que el 802.11 fuera compatible con Ethernet sobre la capa de enlace de datos. En particular, se podría enviar un paquete IP sobre la LAN inalámbrica del mismo modo en que una computadora conectada mediante cable enviaba un paquete IP a través de Ethernet. No obstante, existen algunas diferencias inherentes con Ethernet en las capas física y de enlace de datos y tuvieron que manejarse mediante el estándar. Primero, una computadora en Ethernet siempre escucha el medio antes de transmitir. Sólo si el medio está inactivo la computadora puede empezar a transmitir. Esta idea no funciona igual en las LANs inalámbricas. Para ver por qué, examine la figura 1-36. Suponga que la computadora A está transmitiendo a la computadora B, pero el alcance del radio del transmisor de A es muy corto para encontrar a la computadora C. Si C desea transmitir a B puede escuchar el medio antes de empezar, pero el hecho de que no escuche nada no quiere decir que su transmisión tendrá éxito. El estándar 802.11 tenía que resolver este problema. El segundo problema que se tenía que resolver es que los objetos sólidos pueden reflejar una señal de radio, por lo que ésta se podría recibir múltiples veces (a través de varias rutas). Esta interferencia da como resultado lo que se llama desvanecimiento por múltiples trayectorias. El tercer problema es que una gran cantidad de software no toma en cuenta la movilidad. Por ejemplo, muchos procesadores de texto tienen una lista de impresoras de entre las cuales los usuarios pueden elegir para imprimir un archivo. Cuando la computadora en la que se ejecuta el procesador de texto se coloca en un nuevo entorno, la lista interna de impresoras ya no es útil.

El cuarto problema es que si una computadora portátil se mueve lejos de la estación base que está usando y dentro del rango de una estación base diferente, se requiere algún tipo de manejo. Aunque este problema ocurre con los teléfonos celulares, eso no sucede con Ethernet y requiere solución. En particular, la red prevista consta de múltiples celdas, cada una con su propia estación base pero con las estaciones base conectadas por Ethernet. Desde fuera todo el sistema se vería como una Ethernet sola. La conexión entre el sistema 802.11 y el mundo exterior se conoce como portal.

Protocolos de Red

Cuando le hablamos a otra persona, tenemos que asegurarnos de que ambos compartimos la información y el contexto necesario para que las ideas que expresamos tengan sentido. Como las computadoras no tienen la flexibilidad de la gente, esas conversaciones consisten en mensajes formateados con precisión que se envían las computadoras entre sí siguiendo un modelo estricto y rígido llamado protocolo.

¿Qué es lo que hacen los Protocolos de Red?

Los detalles precisos de lo que hacen los protocolos dependen del tipo de protocolo y de las tareas que les estemos pidiendo a la computadora, pero las funciones generales que cumplen aquellos en nuestra red son comunes:

- Enviar y recibir mensajes de cualquier tipo a través del hardware de la red
- Identificar quien envía y cuál es el destino del mensaje, y determinar si la computadora que recibe es el destino final.
- Para las computadoras con múltiples conexiones de red, enviar si es posible los mensajes recibidos a lo largo del camino hacia su destino final.
- Verificar que el mensaje recibido ha llegado intacto o solicitar la retransmisión de mensajes dañados.
- Descubrir las computadoras que están operando en la red de área local.
- Convertir los nombres de las computadoras en direcciones usadas por el software y hardware de la red y viceversa.
- Publicitar los servicios ofrecidos por esta computadora y solicitar cuales son los servicios ofrecidos por las otras computadoras.
- Recibir la identificación del usuario y la información de autenticación, y el control de acceso a los servicios.
- Codificar y decodificar la información transmitida para mantener la seguridad a través de una red poco segura.

- Transferir información en ambos sentidos de acuerdo a los requerimientos del software y servicios específicos.

1.1.17 ESTUDIO DE CAMPO

En este espacio nos dirigimos a la sede Uniminuto calle 80 en donde vimos las características de los laboratorios de redes, como manejan el diseño físico y lógico, la organización en cuanto a la seguridad de estos y la forma en que realizan las prácticas sus estudiantes.

En cuanto a las características de los laboratorios se asemejan mucho a los que en el presente tiene la sede centro regional Soacha, lo único que los diferencia es que tienen en cada salón un rack en donde guardan los equipos como switch patch panel y patch cord los cuales son utilizados para las prácticas y que cada puerto disponible en los puestos de trabajo quedan sin configuración para realizar cualquier tipo de práctica supervisada por el docente encargado. La topología que manejan es en estrella, un cableado estructurado por medio de canaletas que van empotradas en los escritorios, otro distintivo que se encontró allí es la seguridad con la que se maneja el ingreso a los salones, ya que todo estudiante debe presentar su carnet ante un monitor de laboratorio el cual verifica en el sistema si el estudiante tiene permisos para ingresar al laboratorio dándole así ingreso a su clase o práctica.

En la parte de anexos se encuentran algunas imágenes del laboratorio y su diseño.

2. FASE DE INICIO

2.1 Descripción de la estructura Física del edificio

La estructura del edificio se encuentra construida en concreto, el acceso y salida a este se realiza por medio de dos puertas metálicas, esta distribuido en 5 niveles a los cuales se acceden por una escalera que lleva a cada uno o en la parte exterior por una rampa amplia de concreto y barandas metálicas de acceso que conecta con cada nivel, sus pisos son en baldosa.

En el primer nivel se encuentra las oficinas de bienestar, ciencias básicas comunicación, un cuarto de copiado, una área central descubierta en donde esta la cafetería, se encuentra la biblioteca y dos baños uno de hombres y uno de mujeres.

El segundo nivel cuenta con 6 laboratorios de sistemas un auditorio y las oficinas correspondientes al área administrativa gst y coordinaciones de ingeniería, pisos en tableta dos baños uno de hombres y otro para mujeres.

En el tercer nivel encontramos 5 laboratorios de sistemas una oficina administrativa un cuarto en donde ahí un rack y una conexión de Internet que alimenta a estas salas un baño de hombres y otro de mujeres; además de esto encontramos el salón 311 que corresponde al futuro Laboratorio de Redes y Seguridad Informática, el cual cuenta con una puerta en madera una cerradura común.

En su interior se encuentra tres lámparas de bombillas fluorescentes, una ventana en su parte frontal con vidrios transparentes que aumenta la iluminación del salón las paredes son en ladrillo su piso en tableta roja, en una pared lateral esta el tablero en acrílico blanco.

Seguidamente esta el nivel 4 en donde encontramos salones de clases normales dos baños uno de hombres y otro de mujeres.

Finalmente el quinto nivel consta de salones de clase y se encuentra el techo del edificio el cual esta en teja en buen estado.

2.1.1 Descripción de la estructura eléctrica

El sistema de energía del edificio es prestado por la empresa CODENSA lastimosamente no hay un plano eléctrico para el edificio se sabe de tres cajas que están distribuidas en el edificio las cuales distribuyen la luz, lo importante es que la sala 311 cuenta con suministro además de que cuenta con polo a tierra algo muy importante para el cuidado de los equipos

2.1.2 Descripción de las zonas comunes

El edificio cuenta con una cafetería dotada de 10 mesas para uso público baños escaleras con la debida señalización, en cada nivel encontramos extintores al final de cada escalera y en las oficinas, contando con plan de evacuación ya que la universidad realiza simulacros cada año para prever cualquier caso de emergencia por desastres aunque falta un poco mas de información en las instalaciones sobre los planos de evacuación del edificio.

2.2.2 Requisitos Puntos de red

Para analizar los requisitos necesarios de cada punto de red, tenemos que remontarnos a las normas de cableado estructurado; en especial a la EIA/TIA 568B, 569. 606 y a la IEEE 802.1 hasta 802.11 las cuales darán certificación a cada punto de red instalado, se incluyen materiales necesarios para su instalación como cable, canaleta, conectores, tomas, etc.

Según el diseño a proponer se tiene 14 puestos de trabajo, dos de ellos servidores, los cuales deben tener un mínimo de dos salidas o conectores de red y dos salidas de toma eléctrica por cada puesto de trabajo individual, los dos servidores trabajaran inalámbricamente pero tendrán la opción de conectarse desde el rack a sus tarjetas de red directamente como método de práctica. Los requisitos físicos de un punto de red para la salida de voz y datos son:

- Tarjetas de red para desktop
- Toma de punto de red
- Cable UTP categoría 6
- Conectores RJ45 hembra
- Switch 24 puertos

- Pach cord
- Pach panel
- Rack

Así mismo se tendrá en cuenta que la distancia máxima entre los puntos de red y el Rack de comunicaciones es de 90 mts, según lo establece la norma anteriormente mencionada EIA/TIA 568B.

Se contara con Access point para aumentar la calidad de la señal inalámbrica así ofrecer acceso a internet por medio de la red inalámbrica a usuarios extras como por ejemplo portátiles asegurando prácticas de este tipo.

Para habilitar los puntos de red es necesario realizar su activación en cada puesto de trabajo por medio de su sistema operativo, por la disponibilidad de Uniminuto centro regional Soacha será por medio de Windows XP SP3, ya que solo se tiene licenciamiento para este SO.

Requisitos de crecimiento físico de la red

La escalabilidad mide en qué grado puede un equipo o aplicación aumentar su capacidad y cubrir una mayor demanda de rendimiento, con el fin de que cumpla este objetivo en la red frente al diseño que se ha de proponer, se han de tener en cuenta los siguientes aspectos:

- El primer aspecto importante a evaluar en el crecimiento físico de la red, es el espacio asignado que desde un principio debe tener claras las miras a futuro que se pretendan y con ello se pueda readecuar más adelante con mejores componentes o que la remodelación del mismo no afecte la consecución del estado del laboratorio actual.
- Con respecto al hardware los componentes de conexión como el switch debe permitir la extensión de puertos al colocarlo en cascada sin que baje su velocidad de operación y trabaje en óptimas condiciones según la topología utilizada en él. Además de esto los equipos de trabajo deben tener un estándar en su hardware para así tener la posibilidad de aumento de velocidad si es necesario con la incorporación de sistemas base de mayores requerimientos.

- De igual manera de cuenta con un acces point que cubrirá una mayor área lo cual permitirá la conexión inalámbrica sin necesidad de aumentar los puntos de red. Lo que a futuro permitirá hacer prácticas con tecnologías nuevas como tabletas, Smartphone, ipad y otras que puedan ir apareciendo conforme avance la tecnología.
- Con respecto a los servidores estos deben tener la capacidad de agregar gradualmente uno o varios sistemas de acuerdo al crecimiento de la red en su debido momento, optimizando y mejorando los recursos actuales. Así teniendo en cuenta desde pequeños grupos de trabajo hasta implementaciones de mayor amplitud; lo que conllevaría a que tengan características en su hardware como la de aumento de velocidad con disponibilidad de slots de memoria y aumento de almacenamiento en sus discos duros.
- Al mismo tiempo para permitir un adecuado funcionamiento, crecimiento extenso y correcta interconexión de los diferentes nodos de la red se debe diseñar un plan de direccionamiento que cubra los protocolos de enlace y red, y cumplan con los requerimientos que en el momento se lleguen a necesitar.

2.2.3 Requisitos de seguridad física.

Cuando se habla de seguridad física se hace referencia a los mecanismos de prevención y protección que permiten proteger físicamente cualquier recurso del sistema y el entorno en que se encuentra. Así mismo es necesario contar con niveles de seguridad que cubran áreas comunes, controlen perímetros y entradas físicas e implementación de elementos de seguridad

De acuerdo a lo evaluado en el centro regional Uniminuto Soacha, a continuación se menciona los requisitos mínimos indispensables para el mejoramiento de la seguridad física actual según lo determinan las áreas de control del estándar ISO/IEC 27002.

Entorno o área.

- Las ventanas deben tener protección externa, por medio de una malla de seguridad y película de recubrimiento oscuro que de protección y no permita la visualización interna del laboratorio.

- Contar con un equipo de seguridad apropiado que controle la humedad y la temperatura la cual no debe superar los 25°C, detectores y alarmas de calor, humo y humedad, sistemas de extinción de incendios; la revisión sobre este tipo de equipos debe ser regular de acuerdo con las instrucciones del proveedor.
- Definir reglas de comportamiento para el ingreso al laboratorio como prohibido fumar, prohibido comer en las salas, volumen moderado en la sala etc.
- Documentar debidamente los procedimientos de emergencia y revisar esta documentación de forma regular.
- El piso debe contar con un material antideslizante para prevenir accidentes del personal que interactúa con los equipos

Hardware

- Como componente del sistema más costoso que se encuentra en el laboratorio su prevención con respecto al acceso físico al área debe estar controlado en primer lugar solo podrán ingresar estudiantes y profesores registrados y que en ese momento tengan clase según su horario académico en la sala, además de esto se debe contar con cámaras de vigilancia de circuito cerrado o alarmas.
- Ante la prevención de desastres naturales como los terremotos, es necesario no ubicar equipos en sitios altos para evitar caídas, no permitir colocar equipos móviles sobre los equipos para evitar que se caigan sobre ellos, separar los quipos de las ventanas para evitar que se caigan por ellas u objetos lanzados del exterior que les afecte. Utilizar fijaciones para elementos críticos y colocar los equipos sobre plataformas de goma para que esta absorba las vibraciones.
- Los componentes del sistema deben ir etiquetados con el fin de identificarlos, estos rótulos deben ser fácilmente localizables de acuerdo a su tamaño, color y contraste para el personal que realice trabajos de instalación de nuevos servicios y mantenimiento de la infraestructura de telecomunicaciones; así mismo las etiquetas deben ser resistentes a las

condiciones ambientales del salón y deben tener una vida útil igual o mayor al componente que identifican.

- La instalación eléctrica debe contar con polo a tierra.
- Se debe tener un sistema que controle la sobrecarga de energía como las ups.
- Ante los dispositivos y finalidades del laboratorio se debe contar con implementos que permitan la descarga de la estática del cuerpo humano para así evitar daños irreparables al sistema; (se aconseja el uso de manillas dentro del laboratorio).
- Manejar backups de los sistemas operativos base para atender con prontitud los errores en el sistema y así mantener la sala en óptimas condiciones.
- Los objetos de práctica como routers patch panel conectores deben estar en un gabinete bajo llave y solo se utilizaran bajo supervisión del profesor después de aprobación del laboratorista.

2.2.4 Requisitos lógicos

2.2.4.1 Tipo de información que se transmitirá por la red

La arquitectura de la red está prevista para soportar 14 puestos de trabajo y 2 módulos que serán los servidores; todos estos puestos estarán disponibles para cualquier práctica implementada sobre redes y seguridad, tendrá capacidad para transmisión de voz datos y video.

2.2.4.2 Velocidad y flujo de datos

Uno de los factores más importantes dentro del laboratorio es la calidad con la que se transmite la información, es por ello que se debe garantizar que los

componentes integren estos requisitos para permitir el mejor aprovechamiento de la red Y así los componentes que forman parte de esta, junto con la tecnología utilizada deben permitir satisfacer una demanda inmediata de ancho de banda óptima.

Según todo lo anterior los requisitos mínimos de velocidad y flujo de datos son:

- Tecnología fast Ethernet; esta permite que al utilizar cable utp categoría 5e y 6e se puedan alcanzar fácilmente velocidades de 100 Mbps Base tx.
- Cable utp: categoría 6e para uso interno y categoría 5e si se quiere utilizar para prácticas lo cual logra transmitir a 25Mbps cada par de cable.
- Switch: este componente de la red debe tener la capacidad de generar una velocidad de transmisión igual o mayor a 100 Mbps, permitiendo abastecer cada uno de los puntos de red para la operatividad de la red.

Así con lo anterior el flujo de datos será proporcional a la utilidad y utilización que se le asigne al laboratorio.

2.3.3 Requisitos de seguridad lógica

Es importante para el laboratorio contar con las políticas de seguridad que protejan la información que circule en él, por ello la seguridad lógica que se implementara para él, ira de acuerdo a las practicas que se lleven a cabo y las recomendaciones de las áreas de control del estándar ISO/IEC 27002 de acuerdo a esto se definen los siguientes parámetros:

- Prohibir el acceso a los equipos de red desde el exterior, limitando la posibilidad de denegaciones de servicios o intrusiones no deseadas.
- Filtrar los posibles intentos de IP spoofing que pudieran aparecer.
- Conectar los centros de gestión a la red de una forma transparente, en un entorno de alta disponibilidad y contemplando los requerimientos de las distintas aplicaciones

- Activar un firewall que proteja la red de ataques de intrusos o hackers externos.
- Establecer los preceptos de seguridad de la IAAA para el acceso a todos los equipos, estando la autenticación centralizada en el servidor.

3. DISEÑO DE LA RED

3.1.1 Diseño Físico.

En este capítulo se describe el método con el cual se va a realizar el plan de diseño del laboratorio de redes y seguridad informática del centro regional Uniminuto Soacha, en el cual se van a detallar los componentes que se implementaran en él y la estructura física general del salón, así mismo la distribución de los elementos con los cuales se van a llevar a cabo las prácticas de los diferentes módulos de tecnologías; orientando lo anterior a la mejor utilización y aprovechamiento del espacio.

De acuerdo a la estructura básica de la red del laboratorio se dispondrá de los siguientes componentes:

- **Cableado estructurado:**

En un sistema de cableado estructurado, cada estación de trabajo se conecta a un punto central, facilitando la interconexión y la administración del sistema, esta disposición permite la comunicación virtualmente con cualquier dispositivo, en cualquier lugar y en cualquier momento. Esto garantiza la utilización de diferentes tecnologías en las prácticas sin dañar la red en sí, ya que es la forma más ordenada y adecuada de interconectar varios y diferentes equipos, además de ser de bajo costo es la mejor implementación que puede tener el laboratorio.

Este tipo de sistema esta abalado por los estándares de la ANSI/ TIA /EIA568, ANSI/ TIA/ EIA 569 y la ANSI/ TIA/ EIA/607 lo que hace tender a una estandarización de los sistemas de transmisión de información al integrar diferentes medios para soportar toda clase de trafico y controlar los procesos y sistemas de administración.

Ahora bien se dispondrá de este sistema en el espacio asignado por medio de un tendido horizontal que rodea al salón a través de unas mesas canalizadas, permitiendo la interconexión desde los dos racks o gabinetes que estarán en el centro del aula llevando por medio de una canaleta en el techo hacia las estaciones de trabajo y hacia los dos servidores el cableado, por medio de una topología en estrella; proporcionando así una mejor administración del sistema.

- **Cuarto de Equipos de Red:**

El cuarto de equipos es un espacio centralizado para los equipos de telecomunicaciones (Ej. PBX, Equipos de Cómputo, Switch), que sirven a los ocupantes del edificio. Este cuarto, únicamente debe guardar equipos directamente relacionados con el sistema de telecomunicaciones y sus sistemas de soporte. La norma que estandariza este subsistema es la EIA/TIA 569.

De acuerdo a lo anterior se asignara un espacio dentro del salón, más exactamente en el centro, será delimitado por medio de un panel que servirá como puerta y un candado, tendrá una medida de 210*61*67, estará con su correspondiente señalización evitando que los usuarios manipulen el mismo y puedan ocasionar daños al sistema.

- **Rack:**

También llamados gabinetes o soportes metálicos, es una estructura de materiales resistentes de forma cuadrada, de diferentes tipos acordes a las necesidades de los usuarios. Utilizados para colocar accesorios de conexión para servicios de datos.

Dentro del espacio asignado que será en el centro del salón se contara con un gabinete principal de administración de medidas 210*61*67 puesta acrílico o puerta malla para la ubicación de los componentes (switch, patch panel, patch cord) que permitan la salida de voz datos y video, los cables de interconexión dando la facilidad de llegar a cada una de las áreas de trabajo y módulos respectivos. Se escogió este tipo de gabinete con estas características de acuerdo a la ubicación que tendrá dentro del laboratorio y la facilidad que nos brinda para la manipulación de los componentes.

- **Switch:**

Un switch es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. El switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto. Opera en la capa 2 del modelo OSI y reenvía los paquetes en base a la dirección MAC.

El switch segmenta económicamente la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final. No están diseñados con el propósito principal de un control íntimo sobre la red o como la fuente última de seguridad, redundancia o manejo.

Al segmentar la red en pequeños dominios de colisión, reduce o casi elimina que cada estación compita por el medio, dando a cada una de ellas un ancho de banda comparativamente mayor.

De acuerdo a lo anterior los switch que se utilizaran serán 3 de 24 puertos rackeables para la interconexión de los equipos de las subredes de la red LAN del laboratorio permitiendo la escalabilidad de la red y aprovechando su cantidad de puertos para mejorar las prácticas que se puedan llevar a cabo con estos, uno será fijo y los otros dos estarán disponibles para los estudiantes en su proceso de formación.

Estos Switches soportan Voz, Datos, Video y Acceso Seguro. Ofrecen Una Gestión escalable conforme cambian las necesidades del laboratorio. Manejan las siguientes características:

- Switch Capa 2 con características básicas Capa 3 para la conectividad de acceso empresarial.
- Diseño no-blocking evitando posibles pérdidas de paquetes Múltiples sesiones simultaneas de Administración Priorización de Tráfico capa 4 IEEE 802.3af PoE, ofrece hasta 15.4w por puerto y es compliand 802.3af para alimentar dispositivos como teléfonos, Access Points y Cámaras de seguridad Conectividad de Uplink Gigabit en cobre y Fibra óptica Soporte de Paquetes Jumbo Frames Soporte de protocolos de Alta disponibilidad como 802.3ad Link Aggregation, 802.1s Multiple Spanning Tree y fuentes de poder externas opcionales Administración y gestión via CLI, SNMP,

RMON, XRMON, SFLOW Soporte de dos imágenes de sistema operativo sobre la flash Soporte de VLANS 802.1Q con 256 vlans simultaneas y 4096 Vlans ID Características de seguridad de acceso como 802.1x, Web Based authentication, MAC-base authentication.

- Soporte de funcionalidades de seguridad como ACL, Identity ACL, Dynamic ARP Protection, Source port Filteting, DHCP Protection, STP Root guard que son capaces de protegerse de ataques comunes de intrusos DoS o ataques man in the middle (MITM).
- Soporte de protocolos de convergencia como 802.1AB LLDP y LLDP MED para entregar parámetros como QoS, Vlan configurando dispositivos como los teléfonos IP Soporte de protocolos Multicast para aplicaciones de video o de requerimientos especiales de ancho de banda.
- **Patch Panel**

Los llamados Patch Panel son utilizados en algún punto de una red informática donde todos los cables de red terminan. Se puede definir como paneles donde se ubican los puertos de una red, normalmente localizados en un bastidor o rack de telecomunicaciones. Todas las líneas de entrada y salida de los equipos (ordenadores, servidores, impresoras... etc.) tendrán su conexión a uno de estos paneles.

En una red LAN, el Patch Panel conecta entre sí a los ordenadores de una red, y a su vez, a líneas salientes que habilitan la LAN para conectarse a Internet o a otra red WAN. Las conexiones se realizan con “patch cords” o cables de parcheo, que son los que entrelazan en el panel los diferentes equipos.

Los Patch Panel permiten hacer cambios de forma rápida y sencilla conectando y desconectando los cables de parcheo. Esta manipulación de los cables se hará habitualmente en la parte frontal, mientras que la parte de atrás del panel tendrá los cables más permanentes y que van directamente a los equipos centrales (Switches, Routers, concentradores... etc.).

En el laboratorio se contara con 3 patch panel de las siguientes características:

- Categoría 6E de 24 puertos cada uno

- Cumple con las normas EIA/TIA 568a, 568b.
 - Compatibilidad con las tecnologías de redes
 - Ofrece capacidades de extensión de red fáciles
 - Ideales Para redes Ethernet/ fast Ethernet/ Gigabit Ethernet (1000 Base-T)
 - Compatibles con cableado Categoría 5E
- **Patch Cord:**

Son cables de conexión de red. Su punta termina en un RJ-45 macho. Están contruidos con cable UTP de 4 pares flexible terminado en un plug 8P8C(RJ45) en cada punta de modo de permitir la conexión de los 4 pares en un conector RJ45. A menudo se proveen de distintos colores y con un dispositivo plástico que impide que se curven en la zona donde el cable se aplana al acometer al plug.

Este dispositivo se conectara del patch panel a los Switch para permitir la transmisión de los datos que viajaran por la red y que permitirán la administración de la misma a través del equipo activo, para lo anterior se utilizara cable UTP categoría 6; de igual manera este cable se conectara desde el equipo periférico (pc, impresora o similares) hacia la toma de red de datos ubicada en la canaleta por medio del conector RJ45 así mismo estos deberían ir etiquetados en los extremos para su mejor ubicación.

En cuanto a la distancia que debe tener los patch cord y el patch panel ha de ser de 6 mts y el límite para los patch cord en la conexión del terminal debe ser de 3 mts de acuerdo la norma.

- **Conector RJ-45**

Estos elementos vienen diseñados bajo lineamientos que cumple con las normas finales de la ANSI/ TIA/ EIA 568 A y 568B de acuerdo a la etiqueta de codificación de colores.

En el diseño de la red del laboratorio se utilizaran para la conexión de los canales desde la toma RJ45 hasta los paneles de interconexión.

- **Cable UTP categoría 6E**

El cable de Categoría 6, comúnmente conocido como Cat6, es un cable estándar para Gigabit y todas las redes anteriores, incluyendo 10BASE-T y 100BASE-TX. Todos los cables utilizados, incluyendo Cat5, Cat5e Cat6 comparten la misma estructura básica de cuatro pares de cables retorcidos. La diferencia es la cantidad de datos que cada cable está calificado para transportar.

Los Cableados que cumplen la de categoría 6, o Cat 6 o Clase E (ANSI/TIA/EIA-568-B.2-1) son instalaciones de cableado que cumplen lo especificado en el estándar de cables para Gigabit Ethernet y otros protocolos de redes que son compatibles con versiones anteriores, con los estándares de categoría 5/5e y categoría 3.

La categoría 6 posee características y especificaciones para crosstalk y ruido. El estándar de cable es utilizable para 10BASE-T, 100BASE-TX y 1000BASE-TX (Gigabit Ethernet) y alcanza frecuencias de hasta 250 MHz en cada par. El cable de categoría 6 contiene 4 pares de cable de cobre trenzado, al igual que estándares de cables de cobre anteriores. Un canal completo (cable horizontal más cada final) está permitido a llegar a los 100 metros en extensión.

Para aprovechar al máximo la velocidad de esta tecnología se pretende que el laboratorio quede a la vanguardia y su cableado estructurado pueda aceptar cambios posibles al gran avance tecnológico de hoy en día.

- **Canaleta**

La canaleta es utilizada para la distribución y soporte del cableado, así mismo permite conectar el hardware entre la salida del puesto de trabajo hacia el cuarto de equipos.

La canaleta a utilizar en el laboratorio es plástica 40X16 con separador se instalara con todos sus accesorios y acoples que correspondan al cable UTP cat 6E del cableado, será fijada a las mesas con tornillos en todo su recorrido e interiormente tendrá amarres plásticos para sostener los conductores cada metro.

No es recomendable compartir el cableado eléctrico con el cableado estructurado puesto que genera ruido e interferencias en la transmisión de la información, así que se instalara una canaleta aparte separada 50 cm igual bordeando el área del salón y así evitar que la red se vea afectada en la velocidad de transmisión y el suministro de energía a los equipos. Esta canaleta debe tener puntos de fijación y aseguramiento cada 1 mts.

- **Will Plates**

Estas son las tapas plásticas que se encuentran normalmente en las paredes o canaletas que permiten la conexión de los pcs en la red.

Estos dispositivos son modulares y vienen sin el conector por lo tanto se les debe agregar para realizar la conexión. Depende de la necesidad donde se desee instalar se dispone de Will plates que permiten desde una hasta cuatro diferentes conexiones al mismo tiempo.

De acuerdo con el diseño del laboratorio se cuenta con 14 puntos de red dobles para conexión de red, se utilizaran en los puestos de trabajo, quedando en cada uno un punto libre opcional por si se desea conectar equipos periféricos o accesorios compatibles. Así teniendo la disponibilidad de la red para las prácticas correspondientes según la metodología usada por el docente.

- **Salida Tomacorriente Regulada**

Se tendrán tomas eléctricas dobles con polo a tierra aislado color naranja. En el laboratorio se contara con 17 salidas tomacorriente regulado que serán distribuidas entre los 14 puestos, de trabajo dos cuartos de cómputo y dos servidores

- **Equipos de Computo**

Para el laboratorio de redes y seguridad informática se dispone de 14 equipos para utilización libre y de práctica los cuales cuentan con las siguientes características o especificaciones técnicas:

- Monitor lcd., 4 gb de RAM dd3.
- Disco duro de 500 gb.
- Memoria ddr 3 de 4 gb.
- Unidad óptica quemador DVD.
- Mouse óptico.
- Tarjeta de red LAN y WLAN integrada.
- Salida y entrada de audio.
- Teclado Multimedia.
- Puerto serial integrado.
- Puerto USB 3.0.

La ubicación de estos equipos es de 4 puestos de trabajo en dos costados y 6 en el costado libre dejando así espacio en el centro del laboratorio para mejor utilización y desarrollo de las prácticas.

- **Regulador**

Un regulador de voltaje, proporcionan el voltaje estable que requieren los computadores y demás equipos electrónicos comerciales e industriales, corrigiendo automáticamente las variaciones de la línea de alimentación AC al tiempo que limitan los picos de voltaje, utilizado para ello un sofisticado sistema de supresores.

En la actualidad se cuenta con un regulador de las siguientes características; maneja un voltaje de entrada de 115 VAC+/-20% 2F,N,T. de salida 115 VAC+/-3% 2F,N,T una potencia de 30KVA y una frecuencia de 60 HZ

- **Servidores**

Un servidor es un equipo central el cual administra la conexión hacia los computadores o puestos de trabajo, así mismo gestiona los servicios de (web, correo y bases de datos principalmente).

En el laboratorio se contara con 2 equipos que servirán como servidores con las siguientes características de hardware:

- Procesador Intel® Xeon® X3440 (8MB Caché, 2.53 GHz, Turbo, HT)
- SATA integrado, 1 a 4 Discos Duros conectados al controlador SATA Integrado
- Memoria de 2GB (1X2GB), 1333MHZ SINGLE RANKED UDIMM
- Disco duro SATA 500GB 7.2K RPM 3Gbps 3.5 pulgadas
- Chassis PowerEdge T310 hasta con 4 Disco Duros Cableados y Paquete Cuadruple de LEDs de Diagnóstico
- DVD-ROM (Interno)
- Mouse óptico.
- Tarjeta de red LAN y WLAN integrada.
- Salida y entrada de audio.
- Teclado Multimedia.
- Puerto serial integrado.
- Puerto USB 3.0.

- **Servidor Linux / Windows**

La distribución Linux más común que se utiliza para instalar un servidor es Centos una distro Linux que se basa en Red Hat Enterprise Linux pero que es

totalmente libre y tiene disponible actualizaciones en los repositorios de manera libre y gratuita sin necesidad de pagar el costoso soporte anual por servidor de Red Hat; se escogió este sistema por su fácil mantenimiento, desarrollo activo infraestructura de bajo requerimiento explotando mejor las facultades del hardware al que será instalado, por su seguridad siendo un sistema operativo Unix bajando un 99% virus reales o códigos maliciosos lo que hace que la pérdida de datos sea algo casi desconocido.

Entre las aplicaciones que ofrece se encuentra Open office; suite ofimática libre, picasa que permite el inventario de todos los archivos gráficos y su clasificación, e incluye además herramientas de edición y retoque fotográfico. Samba, programa de código abierto que permite compartir archivos e impresoras desde una computadora Linux hacia una computadora con Windows; servidor freeradius (Remote Authentication Dial-In User server siendo un protocolo AAA (Autenticación, autorización y registro de auditoria) empleado para controlar el acceso a los servicios de red.

Ahora bien el segundo servidor será manejado bajo la plataforma Windows con Windows server se recomienda su versión 2012, por ser la última versión que Microsoft lanzó al mercado la cual permite capacidad de crear grupos de servidores, que son colecciones de servidores que ya existen en la red, y se pueden gestionar a través de la nueva experiencia de usuario. La creación de nuevos grupos de servidores le permite gestionar las tareas entre cada servidor con atributos comunes -un grupo de servidores que contiene todos los equipos que ejecuten IIS, por ejemplo; un grupo de todos los servidores de bases de datos, y así sucesivamente, y proporcionar información específica sobre cualquiera de ellos como desee. Esta es una gran bendición para las organizaciones sin software de monitoreo dedicado. La característica Hyper-V Replica permite replicar una máquina virtual de una locación a otra con Hyper-V y una conexión de red -y sin ningún tipo de almacenamiento compartido. Este es un gran problema en el mundo de Microsoft para la recuperación ante desastres, alta disponibilidad y mucho más. VMware hace esto también, pero el vendedor cobra por las licencias extra de tal capacidad.

Esto hace que mantener en pie las instancias de servicios en todo el mundo sea un asunto de uno o dos clics (suponiendo que existe conectividad de red). Las nuevas interfaces de Hyper-V Replica dentro de Hyper-V Manager incluyen una interface mucho más simple para la creación de una secuencia de replicación, y un mejor control del proceso y de la salud general de los sistemas y socios de replicación, entre otras características que podrán manejar los estudiantes y así estar a la vanguardia de la tecnología del siglo XXI.

Estos servidores estarán en la capacidad de soportar datos, voz y parte de seguridad, estará implementado por medio de una configuración especial en un solo paquete administrable, esto con la intención de instaurar practicas dentro de la operación del laboratorio; prácticas de configuración de servidores y a través de este modelo el participante con la guía docente tendrá la posibilidad de realizar pruebas de configuración manual con la aplicación de protocolos y conceptos de red.

Estos equipos se ubicaran justo detrás de los 2 racks o cuarto de equipos para su utilización en las prácticas aunque tendrán uso restringido ya que solo en clases especiales podrán ser usados.

- **Estructura Modular**

De acuerdo con lo mencionado anteriormente la estructura modular con la que contara el laboratorio se detalla de la siguiente manera:

- **Puestos de trabajo:** Los muebles de computo en el laboratorio constan de 4 mesas rectangulares con medidas de 55 cm de ancho, 3.60 cm de largo y 75 cm de alto en las cuales se encuentran incorporadas las canaletas de tendido eléctrico y cableado UTP con una distancia entre ellas de 50 cm.
- **Cuarto de equipos:** se tendrán dos estructuras modulares en el centro del salón que conformaran un cuarto, diseñados cada uno con un panel que será la puerta el cual tendrá una cerradura que proporcione seguridad a los equipos allí guardados.

- **Seguridad Física General**

En este espacio se describen los elementos correspondientes a la seguridad física que se proponen para generar el soporte necesario al laboratorio y permitir que este se optimice en cada momento de mejor manera:

- **Película Protectora:** esta película es para recubrir la superficie de las ventanas y no permitir la visibilidad del laboratorio y sus componentes es oscura y estará a las medidas de las ventanas para que se adhiera a ellas para dar apariencia de vidrios polarizados.

- **Cerradura de Seguridad** se adaptara para brindar seguridad al ingreso y salida del laboratorio. Estas llaves serán manipuladas únicamente por el administrador de los laboratorios al igual que el acceso al cuarto de equipos.

 - **Rótulos:** Adicional para tener un mayor control y una mejor identificación de los equipos se colocaran marquillas o rótulos con numeración en los extremos de cada cable UTP o en los patch cord, esto con el fin de poderlos identificar en el rack y en la salida de los patch panel y a la llegada de los switches.
- **Pruebas de cableado**

Para comprobar que el montaje y tendido del cableado se encuentra en perfecto funcionamiento para las condiciones del laboratorio y las necesidades del mismo se deben contar con los valores límite para las pruebas de certificación en categoría 6e.

- Atenuación 35.9
- NEXT 33.1
- ELFEXT 15.3
- PSELFEX 12.3
- Return loss 8.0
- Retardo 536.0

De igual manera los siguientes aspectos se deben tener en cuenta para corroborar su buen funcionamiento.

- Conectividad punto a punto
- Longitud del cable

3.1.2 Modulo Cableado

La presencia de este módulo en el laboratorio va a permitir establecer y estructurar las prácticas que comprendan a este tipo de elementos del cableado, adicionalmente la organización del mismo se hará de acuerdo a los elementos que actualmente la Universidad por medio de la facultad ha adquirido.

Se aclara que la estructura física del mismo que corresponde a los materiales se guardara en el gabinete de los elementos mencionados en el diseño general esto para permitir que el profesor encargado tenga la facilidad de disponer de los mismos y así se pueda dar la explicación del laboratorio realizando las conexiones físicas que requieren el trabajo de los estudiantes y en los puestos de trabajo si es necesario realicen las pruebas correspondientes que complementen la práctica, con esto se pasa a la descripción de los componentes del módulo y funcionalidad de los mismos para la realización de las diferentes prácticas.

Los elementos con que cuenta la universidad para la implementación del laboratorio y desarrollo de prácticas se encuentran en ANEXO TABLAS.

Siendo así con los componentes de este módulo se da la posibilidad de soportar prácticas de conexión de cableado, comprendiendo desde la preparación del cable y su ponchado hasta la posibilidad de verificar su funcionamiento y transmisión en una redes datos LAN por medio de los dispositivos que permiten este tipo de transmisión y con esto dar una visión más clara y acorde a las redes de computadores a los participantes del laboratorio, también queda abierto para otras prácticas como mantenimiento de computadores para programas técnicos; todo lo anterior se controla bajo las normas internacionales indicadas para cableado en el presente documento.

Referente al tópico de seguridad informática del programa en este módulo por medio de las practicas se permitirá identificar las falencias que se pueden presentar en las conexiones de cableado estructurado y con base en esta información dar paso a la propuesta de alternativas que minimicen los riesgos de las mismas y a su vez retroalimentar la operación del laboratorio para que cada vez las practicas se puedan llevar a cabo en forma óptima.

3.1.3 Modulo Inalámbrico

Dentro de la estructura del laboratorio se involucra este segundo módulo que establece las conexiones del tipo inalámbrico de gran importancia y auge en estos

momentos en las redes a nivel mundial, con la implementación de esta tecnología se da paso a prácticas que ofrecen la posibilidad al alumno de interactuar con los componentes para complementar su conocimiento teórico; todos los elementos correspondientes a la tecnología inalámbrica se almacenaran en los dos gabinetes en el cuarto de equipos o rack.

Así los docentes encargados de las materias correspondientes al software y hardware inalámbrico disponer de los elementos y a su vez del traslado de estos dentro del salón para la cobertura necesaria y dar respuesta a los requerimientos de los trabajos a establecer en estas clases, a continuación se nombran los elementos disponibles por la universidad para la aplicabilidad del laboratorio:

- **Router Inalámbrico linksys E4200**

Este Router está recomendado para casas muy grandes, con varias estancias y salas de cine. velocidad inigualable y Calidad de Transmisión en HD/3D para disfrutar de la mejor experiencia de Juego y Cine en Casa Que se Pueda Tener lo que supondría una gran calidad de transmisión para las prácticas de acceso remoto y demás que se realicen.

Características:

- Doble banda N Simultánea (2,4 y 5 GHz)
 - Switch Gigabit Ethernet de 4 Puertos
 - Máxima VELOCIDAD: Hasta 300 + 450 Mbp
 - Puerto USB párrafo Almacenamiento Compartido
 - Servidor multimedia UPnP AV Integrado
- **Acces Point**

Un Access Point es un punto de acceso inalámbrico privado, para conectar sus computadoras a Internet sin necesidad de cables, permitiendo compartir recursos de red.

– **ventajas**

- La instalación es flexible debido a que no se necesita cableado.
- La conexión al AP es mediante clave de acceso, impidiendo la piratería.
- El usuario captura datos y accede a la información en tiempo real, permitiendo movilizarse por toda el área de cobertura.
- El protocolo WEP (Wired Equivalent Privacy, Privacidad Equivalente al Cable), es el algoritmo opcional de seguridad que garantiza la privacidad de todas las conexiones inalámbricas.

• **características técnicas**

- Opera en el estándar inalámbrico IEEE 802.11g.
- Velocidad de transferencia máxima de 11 Mbps y se ajusta automáticamente en función de la cobertura y calidad de la transmisión.
- Facilidad de auto instalación y fácil configuración.
- Capacidad de encriptación de las comunicaciones.
- Alcance de 50 m en interiores y 200 en exteriores, aunque estas mediciones son simples referencias ya que el alcance real vendrá determinado por el entorno físico en el que se instale.
- Puede soportar hasta 6 equipos inalámbricos para una navegación óptima constituidos como una red local (LAN) inalámbrica.

En el laboratorio se tendrán 2 de estos equipos, para uso de prácticas y como estación fija para la conexión inalámbrica dentro del laboratorio.

Los equipos de trabajo disponen cada uno de tarjetas inalámbricas lo que asegurara la conexión por este medio entre ellos y los servidores al igual que con las estaciones como router y switch en los racks.

Con respecto a la seguridad informática en este tipo de conexiones es de gran importancia contar con políticas de seguridad que proporcionen confidencialidad, integridad y disponibilidad a la información, es así que aparte de las implementaciones que el laboratorio tendrá en su diseño lógico y seguro del participante del laboratorio va a tener la posibilidad de que por medio de los componentes y su conexión pueda detectar las vulnerabilidades que contenga una red y así plantear alternativas que permitan dar solución a las mismas, basado en los conceptos del tema de la seguridad y a su vez tendrá la facilidad de verificarlos en el mismo laboratorio obteniendo resultados de su experiencia investigativa.

3.2.1 Diseño Lógico

Para llevar a cabo el diseño físico expuesto anteriormente es necesario tener un diseño lógico de la red el cual nos permita establecer cada una de las políticas necesarias de la red LAN para estructurar las diferentes clases de interconexiones de las tecnologías, y así mismo tener las condiciones suficientes para establecer la seguridad, evitando que con las practicas que se lleven a cabo se altere el funcionamiento del laboratorio es decir que de forma libre se puedan ejercer ataques sin que la información se vea afectada.

3.2.2 Arquitectura de la Red

Así de esta manera para la red del laboratorio se estructurará una arquitectura soportada en una topología estrella, esto ya que se considera que de acuerdo a su funcionamiento y distribución es la ideal para las condiciones de manejo de las practicas que se llevaran a cabo en ella.

Junto a la topología de red se tienen 16 puntos de red distribuidos de la siguiente manera:

- Dos puntos de red serán de uso exclusivo de los servidores para garantizar la integridad de la información de la red y mantenerse en línea con los puestos de trabajo.
- 14 puntos de red distribuidos en los puestos de trabajo sobre los cuales se soportaran las prácticas lógicas de software y verificación de funcionamiento de conexiones, con ello junto con las dos máquinas de

servidor podrán estar en línea sobre la topología propuesta para dar solución a los requerimientos de cada uno de los usuarios.

- De igual manera en los puestos de trabajo se tendrán igual número de puertos libres para dar la opción de incluir equipos extras de acuerdo a la disponibilidad de la práctica y los requerimientos que el docente plantee, de igual manera estarán protegidos por la gestión de los servidores.

3.2.3 Direccionamiento IP

La identificación lógica de los equipos activos se debe realizar por medio de la asignación de direcciones IP, configurando los parámetros requeridos para la interconexión y servicios de red.

La asignación de direcciones IP se realizara a través del protocolo DHCP, implícito dentro del sistema operativo Windows Server y Centos, los cuales serán los encargados de establecer las direcciones IP dinámicas de los equipos activos en la red; el laboratorio estará dividido en dos sub redes, cada una controlada por un servidor, esto para realizar las diferentes practicas entre Windows y Linux, pero a su vez estarán interconectadas las dos redes por medio del switch. Esta consecución se propone ya que con base a las diferentes tecnologías que trabajaran sobre la red y de acuerdo al flujo de datos de transmisión es de mejor manejo para las practicas contar con direcciones dinámicas tanto por costos como utilización de esto, para proponer una práctica que por medio de la ayuda del docente oriente al estudiante en la obtención de la administración y manejo de un DHCP.

Según lo anterior el tipo de red que se utilizara será clase C, dado que el espacio de direccionamiento tiene el propósito de admitir redes pequeñas con 254 host como máximo. El rango asignado para los elementos del laboratorio está comprendido entre 192.168.1.0 hasta 192.168.1.254, sin tener algún límite establecido para un número determinado de equipos, igual a la red LAN inicial esta propuesta en condiciones pequeñas con crecimiento futuro.

La red LAN del laboratorio tendrá acceso a internet ya que la universidad cuenta con una IP pública asignada, y ya es de manejo que todos sus laboratorios cuente con este servicio útil en la actualidad para la consecución de las prácticas y el manejo de las clases en el laboratorio.

Y así con los dos servidores conectados en topología estrella con las subredes y asignado por IP dinámicas se permita ver cómo se puede ingresar de una maquina a otra y verificar el tráfico de la misma, simulando de esta forma conexiones a internet.

3.2.4 Métodos de Acceso

De acuerdo a las condiciones con las cuales se va a desarrollar el laboratorio y según las diferentes prácticas que se van a llevar a cabo los usuarios deben contar con la posibilidad de acceder a cada una de las actividades a realizar sin que la red vaya a sufrir colapsos de información o retrasos de transmisión, para que se pueda dar cumplimiento a este requerimiento los puestos de trabajo y equipos activos de la red deben contar con el control de tráfico y así mismo evitar que los paquetes de datos choquen y sean destruidos, el establecimiento de estas reglas es lo que se conoce como métodos de acceso, los cuales cumplen con la función de prevenir el acceso simultaneo en la red.

Al mismo tiempo para dar cumplimiento a su función hay dos métodos de acceso de uso general en redes de área local.

- El acceso aleatorio o contención: Este método permite que cualquier usuario empiece a transmitir en cualquier momento siempre que el camino o medio físico no esté ocupado.
- El acceso determinístico: Con esta cada estación tiene asegurada su oportunidad de transmitir siguiendo un criterio rotatorio.

De acuerdo a las políticas de la red Ethernet que se implementara en el laboratorio y teniendo en cuenta el número de puestos de trabajo se plantea en el diseño lógico la operatividad del método de acceso aleatorio o de contención, esto porque la red de acuerdo a su topología en estrella comparte el medio de transmisión y es necesario que todos los equipos se vean en red, con este método la señal se propaga por toda la red y llega a todos los computadores; es decir por medio del broadcast, operando bajo el principio de escuchar antes de hablar; de esta manera en la red cuando un puesto de trabajo quiera enviar un dato primero se verifica si en el canal alguien está transmitiendo si es así se espera hasta que quede libre en caso contrario se transmite contando con esta posibilidad permanentemente, por lo tanto no se tiene ninguna restricción como en el otro método el cual recorre la

red y organiza la señal para dar paso a la transmisión, en ese orden haciendo más demorado el proceso de entrega de los datos.

Para este tipo de red que debe permanecer en línea constantemente es necesario que el canal permanezca en disponibilidad para la transmisión de los datos, por ello se utilizara este método de acceso CSMA (acceso Múltiple Sensible a la portadora) el más común diseñado dentro del grupo de contención.

Ahora bien si dos computadoras transmiten al mismo tiempo habrá colisión pero para dar solución a esto se contara con el protocolo CSMA el cual opera su funcionamiento en tres fases en las cuales el emisor:

- Verifica que la red esté disponible para transmitir
- Transmite el dato
- Espera verificación por parte del receptor para comprobar que el mensaje haya quedado entregado correctamente.

Con lo anterior se confirma la entrega del mensaje y garantiza la administración del tráfico de red, la cual en el laboratorio según su operatividad es muy importante se corrobore que el dato quede correctamente transmitido y en el caso contrario el canal reenvía el dato de nuevo hasta lograr su destino final, además bajo las condiciones de transmisión de la información de las practicas que se dará en envíos de información normales se puede garantizar con este método de acceso que pocas veces ocurran colisiones y también que hasta que no se entregue de forma total los datos no se terminara el proceso.

3.2.4 Diagrama Lógico De La Red

Este comprende la topología que maneja el laboratorio se encuentra en la lista de anexos lista de figuras, figura 5.

3.3 Selección y Evaluación de Tecnologías

Para el laboratorio de Redes y seguridad informática se tienen por el análisis hecho las siguientes tecnologías las cuales permiten el mejor manejo de este en cuanto a velocidad de transmisión de datos disponibilidad técnica y perdurabilidad:

- **Ethernet:**

Se escogió esta tecnología ya que permite un buen equilibrio entre velocidad, costo y facilidad de instalación. Estos puntos fuertes, combinados con la amplia aceptación en el mercado y la habilidad de soportar virtualmente todos los protocolos de red populares, hacen a Ethernet la tecnología ideal para la red de la mayoría de usuarios de la informática actual lo que proporciona al laboratorio un estándar en cuanto a calidad y compatibilidad con futuros cambios que puedan ocurrir en el interior de él, además que permite la interconexión de:

- NIC, o adaptador de red Ethernet permite el acceso de una computadora a una red. Cada adaptador posee una dirección MAC que la identifica en la red y es única. Una computadora conectada a una red se denomina nodo.
- Repetidor o repeater aumenta el alcance de una conexión física, disminuyendo la degradación de la señal eléctrica en el medio físico.
- Concentrador o hub funciona como un repetidor, pero permite la interconexión de múltiples nodos, además cada mensaje que es enviado por un nodo, es repetido en cada boca del hub.
- Puente o bridge - interconectan segmentos de red, haciendo el cambio de frames (tramas) entre las redes de acuerdo con una tabla de direcciones que dice en que segmento está ubicada una dirección MAC.
- Enrutador o router funciona en una capa de red más alta que los anteriores el nivel de red, como en el protocolo IP, por ejemplo -- haciendo el enrutamiento de paquetes entre las redes interconectadas. A través de tablas y algoritmos de enrutamiento, un enrutador decide el mejor camino que debe tomar un paquete para llegar a una determinada dirección de destino.
- Conmutador o Switch funciona como el bridge, pero permite la interconexión de múltiples segmentos de red, funciona en velocidades más rápidas y es más sofisticado. Los switches pueden tener otras funcionalidades, como redes virtuales y permiten su configuración a través de la propia red.

Lo anterior permite llevar a cabo cualquier práctica suministrada por el programa de la facultad sin necesidad de hacer cambios buscos en el laboratorio o entorpecer la comunicación central de este.

- **Cableado Estructurado:**

El objetivo fundamental es cubrir las necesidades de los usuarios durante la vida útil del laboratorio sin necesidad de realizar más tendido de cables, permite interconectar equipos activos, de diferentes o igual tecnología permitiendo la integración de los diferentes servicios que dependen del tendido de cables como datos, telefonía, control, por lo anterior y por normatividad es indispensable el desarrollo de esta tecnología en la consecución del laboratorio determinada así como de gran importancia para una implementación de red.

- **Redes de área local sin cables (WLANs)**

La tecnología Wlan implementada en el laboratorio garantiza la consecución de las practicas llevándolas a nivel inalámbrico, el aprovechamiento del espectro dando así la posibilidad de interconectar un sinnúmero de equipos aumentando la capacidad de las redes que se podrán manejar cumpliendo así con un nivel de educación conforme la actualidad de las redes lo concierne.

- **Topología En Estrella**

Se utiliza sobre todo para redes locales. La mayoría de las redes de área local que tienen un enrutador (router), un conmutador (switch) o un concentrador (hub) siguen esta topología. El nodo central en estas sería el enrutador, el conmutador o el concentrador, por el que pasan todos los paquetes. Dado su transmisión, una red en estrella activa tiene un nodo central activo que normalmente tiene los medios para prevenir problemas relacionados con el eco. Para aumentar el número de estaciones, o nodos, de la red en estrella no es necesario interrumpir, ni siquiera parcialmente la actividad de la red, realizándose la operación casi inmediatamente.

Según lo anterior es la topología de mejor utilidad para el laboratorio ya que la finalidad de este es ofrecer en sus prácticas conexión sin interrupciones y que

no se vea afectado en su estructura inicial para que manteniéndose así en buen estado y con una disponibilidad de acceso en todo momento.

3.3.1 Software

El software instalado en el laboratorio está orientado de acuerdo a las diferentes prácticas y su comportamiento por ello este se fundamenta como la plataforma lógica sobre la cual se evaluarán los diferentes tipos de datos a transmitir de las tecnologías y además también estableciendo las condiciones de acceso de los equipos generales y la implementación de políticas de seguridad que permitan soportar la red y entregar el grado de protección a la información requerido para su operatividad. De acuerdo a las condiciones con las cuales opera el software se enuncian los diferentes procesos y equipos de la red sobre los cuales operara, describiendo la elección de cada uno de las diferentes instrucciones acorde al funcionamiento y necesidad del área en mención:

- **Sistema Operativo:**

Se utilizara para el diseño de la red dos plataformas Linux y Windows, como anterior mente fue mencionado un servidor bajo Windows y otro bajo Linux (CENTOS), los equipos de trabajo dispondrán también de un sistema base Windows en este caso su versión XP ya que es la licencia con la que cuenta la universidad pero dejando como propuesta para estar a la vanguardia de la tecnología actual un Windows 7 ya que es el actual utilizado en las empresas; en cuanto a Linux se tendrá instalado como base el sistema operativo Ubuntu. Se escoge este porque es el más popular de las plataformas UNIX lo que hace que el manejo de este sea muy cómodo y los estudiantes comiencen a entra en el SL con la versión hecha para hogares.

Entre las características de estos Sistemas operativos encontramos la posibilidad de crear cuentas de usuario, asignar recursos, directorio activo con la capacidad de administrar toda la infraestructura de la red y manejo de procesadores múltiples lo que dará un mejor rendimiento en cuanto a velocidad y seguridad en la red del laboratorio.

- **Antivirus**

Para dar soporte y prevenir la entrada de virus a la red del laboratorio se opta por la opción de un antivirus, la Universidad cuenta con licencia para el antivirus Symantec, el cual cuenta con protección contra acceso a aplicaciones, que restringe el acceso al registro, los archivos, las carpetas y los procesos, cuenta con la capacidad para bloquear una aplicación sospechosa; Firmas genéricas: Protección basada en vulnerabilidades; una sola firma puede detectar cientos de amenazas nuevas. Bloqueo de comportamiento: Analiza el comportamiento de las aplicaciones (aplicaciones conocidas y desconocidas). El bloqueo de comportamiento ofrece una detección más precisa sin la necesidad de instalar configuraciones basadas en normas y sin tener que preocuparse de falsos positivos, todo lo anterior da certeza de confianza respecto a la seguridad de la información que se ingresa y sale del laboratorio.

- **Programas de Gestión de redes y seguridad Informática**

El laboratorio debe contar con programas que funcionen para realizar prácticas además de las que se pueden lograr con los sistemas operativos Windows y Linux ya instalados es necesario la disponibilidad de los siguientes programas que ayudaran en el proceso de utilización del laboratorio:

- **BackTrack:** Es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática. Incluye una larga lista de herramientas de seguridad listas para usar, entre las que destacan numerosos scanners de puertos y vulnerabilidades, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless. Fue incluida en el puesto 7 de la famosa lista "Top 100 Network Security Tools" de 2006. Backtrack le ofrece al usuario una extensa colección de herramientas completamente usables desde un Live CD o un Live USB por lo que no requiere una instalación para poder usarse. O bien, se ofrece la opción de instalar en un disco duro. Entre las herramientas ofrecidas se encuentran:
 - Aircrack-ng, Herramientas para auditoría inalámbrica
 - Kismet, Sniffer inalámbrico
 - Ettercap, Interceptor/Sniffer/Registrador para LAN

- Wireshark, Analizador de protocolos
- Medusa, herramienta para Ataque de fuerza bruta
- Nmap, rastreador de puertos

Y una larga lista de otras herramientas, que se agrupan en 11 familias:

- Recopilación de Información
- Mapeo de Puertos
- Identificación de Vulnerabilidades
- Análisis de aplicaciones Web
- Análisis de redes de radio (WiFi, Bluetooth, RFID)
- Penetración (Exploits y Kit de herramientas de ingeniería social)
- Escalada de privilegios
- Mantenimiento de Acceso
- Forenses
- Ingeniería inversa
- Voz sobre IP

Cabe destacar que siempre se le pueden añadir más herramientas y software libre para desarrolladores de programación, herramientas de oficina, etc. Que originalmente no trae Backtrack, por otro lado también los creadores de esta distro pueden personalizar a gusto el backtrack.

- **packet tracer:** Es la herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA. Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Packet Tracer se enfoca en apoyar mejor los protocolos de redes que se enseñan en el currículum de CCNA. Este producto tiene el propósito de ser usado como un producto educativo que brinda exposición a la interfaz comando – línea de los dispositivos de Cisco para practicar y aprender por descubrimiento. Packet Tracer 6.0 es la última versión del simulador de redes de Cisco Systems, herramienta fundamental si el alumno está cursando el CCNA o se dedica al networking. En este programa se crea la topología física de la red simplemente arrastrando los dispositivos a la pantalla. Luego clickando en ellos se puede ingresar a sus consolas de configuración. Allí están soportados todos los comandos del Cisco OS e incluso funciona el "tab completion". Una vez completada la configuración física y lógica de la net, también se puede hacer simulaciones de conectividad (pings, traceroutes, etc) todo ello desde las mismas consolas incluidas. Una de las grandes ventajas de utilizar este programa es que

permite "ver" (opción "Simulation") cómo deambulan los paquetes por los diferentes equipos (switchs, routers, etc), además de poder analizar de forma rápida el contenido de cada uno de ellos en las diferentes "capas".

- **Apache:** Es el software para servidores tal vez más utilizado en Internet y es el complemento perfecto para crear sitios con PHP y MySQL, es muy poderoso aunque en sitios grandes puede consumir recursos en exceso sin dejar de ser estable, se puede utilizar con infinidad de bases de datos y lenguajes de programación.

Es gratuito y lo puedes descargar compilado para diferentes distribuciones de linux, windows o mac.

- **F.I.R.E.:** Destaca dentro de las distribuciones linux específicas para informática forense.
- **WinHex:** Software para informática forense y recuperación de archivos, Editor Hexadecimal de Archivos, Discos y RAM
- **Encase:** Herramienta propietaria, la cual ha demostrado ser un dispositivo útil a los peritos forenses en diferentes casos.
- **Ossim:** Herramienta de monitorización
- **Nessus:** Otro proyecto para scanear vulnerabilidades
- **Fport:** Identifica puertos abiertos y aplicaciones asociadas a ellos.
- **Stunnel:** Programa que cifra las conexiones TCP bajo SSL
- **AirSnort:** Herramienta wireless para recuperar claves cifradas
- **Aircrack:** sniffer y WEP craqueador de wireless

- **Achilles:** Herramienta para testear la seguridad de las aplicaciones web
- **NetStumbler** Localizador de los puntos de acceso wireless (debes poseer tarjeta wireless para q funcione)
- **Dsniff:** sniffer
- **VNC** Administrador remoto
- **The Autopsy:** Browser para la informatica forense
- **PyFlag:** Herramienta para recuperar discos en RAID

4. Presupuesto

El presupuesto comprende a la inversión que ha hecho El centro Regional Uniminuto Soacha para la implementación del Laboratorio de Redes y seguridad Informática el cual se puede observar en el punto 7 que se refiere a los anexos en donde están las tablas con los datos correspondientes a este punto.

5. Conclusiones

Con la implementación del laboratorio de Redes, la Corporación Universitaria Minuto de Dios regional Soacha, tendrá la capacidad de realizar prácticas a nivel de los programas de Ingeniería de Sistemas modalidad a distancia, Tecnología en Electrónica, Tecnología en informática, Tecnología en Redes y Seguridad Informática, Técnicos, específicas en infraestructura de telecomunicaciones, redes de computadores y configuración de sistemas de Redes LAN y WAN, además esta infraestructura permitirá soportar las tendencias de la tecnología, tanto en el campo de aplicaciones en equipos electrónicos, sistemas WIFI, VLAN, entre otros.

Este diseño físico será un referente para marcar una diferencia entre un laboratorio Informático y un laboratorio de Redes, en donde su principal finalidad no es recibir clases teóricas, si no también ofrece la posibilidad de manipular su ambiente para ir a la práctica necesaria complementando la calidad de formación brindada en el Centro Regional Soacha Uniminuto, abriendo así puertas a sus estudiantes para su vida laboral o su continuación en el conocimiento ya que con un laboratorio específico nuevas carreras o especializaciones relacionadas con las redes comunicaciones y seguridad informática entraran a ser parte de las posibilidades que ofrece la universidad ampliando el conocimiento infundado en ella y lo más importante el valor adquirido al ser un egresado de tan prestigioso y apetecible sitio de formación educativo.

Es necesario por parte de los estudiantes conocer el proceso que se tiene al analizar un laboratorio ya que gracias a este se complementa todo lo aprendido en el transcurso de la carrera de Redes, tomándolo así como una práctica personal en donde se acumula conocimiento que tal vez se cree menos importante pero que en realidad es la esencia de lo que se significa ser Tecnólogo en Redes y Seguridad Informática ya que es la mejor manera de recorrer todo lo aprendido antes de culminar con el pensum educativo ofrecido y recibir un conocimiento completo y con miras a un futuro renovador y prometedor.

6. BIBLIOGRAFIA Y WEBGRAFIA

BIBLIOGRAFIAS

- ANDREW S TANEMBAUM; Redes de Computadores cuarta edición. México: Pearson Educación. 2003. 912p
- SEGURA GARZON; María Roció y GARCIA VALERO, Julián Andrés. Diseño e implementación Laboratorio de Redes. Bogotá. Corporación Universitaria Minuto de Dios. Julio 18 de 2007. 79p.
- CARLOS VARELA, LUIS DOMINGUEZ, Redes inalámbricas Escuela Técnica Superior de Ingeniería Informática Universidad de Valladolid. 2002 18 p.
- RODRIGO ALARCON AVILA, Seguridad en redes como eje temático de investigación, 2007 173 p.
- ING. MARIA ANDREA MORA Tecnologías para redes LAN inalámbricas, Universidad Rafael Belloso Chacin. Venezuela enero-junio 2004 16p.

WEBGRAFIAS

- BACK TRACK LINUX; 2011. <http://www.backtrack-linux.org/>
- MICROSOFT; 2012.
<http://www.microsoft.com/OEM/es/products/servers/Pages/windows-server-2012-overview.aspx#fbid=3pAbm5otW4S>
- SAYA COMUNICACIONES S.A.C - IDG COMUNICACIONES; 2009
<http://cioperu.pe/articulo/11028/diez-caracteristicas-de-windows-server-2012-para-los/>
- IEEE; 2013 <http://www.ieee.org/index.html>
- ISO; 2013 <http://www.iso.org/iso/home.html>
- JEDD KIOSKEA, Creación de una red de área local, 16/10/2008
<http://es.kioskea.net/>
- SKINPRESS NORMATIVIDAD INDUSTRIAL, estandarización, 25/09/2009
<http://normatividadindustrial.com/norma-tiaeia-568-b/>

7. ANEXOS

COSTOS FACTIBILIDAD ECONOMICA

CANTIDAD	DESCRIPCION	VALOR UNITARIO	VALOR TOTAL
2	Rack piso, abierto, altura 45U (210 cm), aluminio.	465.000	930.000
1	Gabinete rack piso, altura 45U (210*61*67), puerta acrílico o puerta malla	1.300.000	1.300.000
2	Bandeja deslizable para Gabinete o Rack (altura 45U)	150.000	300.000
3	Patch panel cat. 6, 24 puertos	153.000	459.000
4	Organizador de cables horizontal para gabinete o rack	40.000	160.000
3	Switch 24 puertos rackeable, no administrable	450.000	1.350.000
3	Router, no administrable	170.000	510.000
14	Equipos de cómputo (monitor lcd, dd 500 Gb, RAM 4 Gb)	900.000	12.600.000
1	Tablero con división 12 circuitos	170.000	170.000
2	Servidores (Linux - Windows). Ref. tabla 2	2.476.002	4952004
1	Kit academia Cisco: CCNA DISCOVERY & CCNA EXPLORATION PREMIUM POD – CISCO 2901. Ver anexo Academias oferta mayo CCNA.doc	10.387.423	10.387.423
1	Router Inalámbrico linksys E4200	389.744	389.744
2	Acces point - Repetidor inalámbrico Wifi 300 Mbps o superior	172.000	344.000
2	Armarios metálicos, puertas batientes, con chapa 1.80 de alto, 0.90 de ancho, 0.45 de profundidad para almacenamiento de equipos	Aprox. 800.000	1.600.000
		SUBTOTAL	\$35.452.171
		IVA	\$5672347,36
		TOTAL	\$41.124.518

TABLA 1 EQUIPOS ACTIVOS

Servidor en torre Power Edge 11G T310

Procesador	Intel® Xeon® X3440 (8MB Caché, 2.53 GHz, Turbo, HT)
Sistema operativo	Sin Sistema Operativo
RAID	Sin RAID - SATA Integrado, 1 a 4 Disco Duros conectados al controlador SATA Integrado
Memoria	Memoria de 2GB (1X2GB), 1333MHZ SINGLE RANKED UDIMM
Disco duro	Disco duro SATA 500GB 7.2K RPM 3Gbps 3.5 pulgadas Cabled
Chasis	Chassis PowerEdge T310 hasta con 4 Disco Duros Cableados y Paquete Cuadruple de LEDs de Diagnóstico
Unidad óptica	DVD-ROM (Interno)

Tabla 2. Especificaciones técnicas del servidor

CANTIDAD	DESCRIPCION	VALOR UNITARIO	VALOR TOTAL
8	Multitoma polo a tierra horizontal	33.000	264.000
12	Anclajes para Rack	12.900	154.800
10	Paquete x 100 conectores RJ45	20.000	200.000
16	Canaleta con separador 40X16	50.000	800.000
20	Faceplate	3.100	62.000
20	Jacks RJ-45	3.900	78.000
25	Tapas troqueladas para electricidad	2.700	67.500
20	Tapas para datos	2.700	54.000
25	Tomas dobles leviton cat 6	10.000	250.000
1	Caja cable UTP cat 6 o superior, uso interior. (305 metros)	300.000	300.000
5	Rollos cinta Aislante 3M	3.000	15.000
100	Metros cable eléctrico trifilar 3X12	4.000	400.000

1	Ponchadora de impacto para RJ45	50.000	50.000
1	Kit instalación (100 chazos puntilla, 3 brocas tungsteno, ½", ¼")	14.550	14.550
1	Kit tornillos para metal (1000 unidades)	30.000	30.000
		SUBTOTAL	\$2.739.850
		IVA	\$438376
		TOTAL	\$3.178.226

Tabla 3. Accesorios y herramientas

CANTIDAD	DESCRIPCION	VALOR UNITARIO	VALOR TOTAL
1	Otros Imprevistos. Para la implementación del laboratorio es necesario asignar un presupuesto adicional en accesorios y herramientas requeridos.	1.000.000	1.000.000
		TOTAL	\$1.000.000

Tabla 4. Otros imprevistos.

CANTIDAD	DESCRIPCION	VALOR UNITARIO	VALOR TOTAL
	Tabla 1. Activos fijos.	TOTAL	\$41.124.518
	Tabla 3. Accesorios y herramientas	TOTAL	\$3.178.226
	Tabla 4. Imprevistos	TOTAL	\$1.000.000
		TOTAL	\$45.302.744

Tabla 5. Precios Totales

--	--

ITEM	NOMBRE EQUIPO	REFERENCIA	COD UNIMINUTO	COD BARRAS	ESTADO ACTUAL	DE BAJA
1	Fuente de alimentación	GPC-3030D	2002032	EG832841	Bueno	No
2	Fuente de alimentación	GPC-3030D	2002034	EG844350	Aceptable	No
3	Fuente de alimentación	GPC-3030D	2002035	EG844352	Deficiente	No
4	Fuente de alimentación	GPC-3030D	2002033	EG832825	Bueno	No
5	Fuente de alimentación	GPC-3030D	2002080	EG832826	Aceptable	No
6	Fuente de alimentación digital	1745A DC	2011626	174510574051115	Bueno	No
7	Fuente de alimentación digital	1745A DC	2011625	1,74511E+17	Bueno	No
8	Generador de señales digital	ECFG-2110	2011623	EK912748	Bueno	No
9	Generador de señales digital	ECFG-2110	2011624	EK912783	Bueno	No
10	Generador de señales digital	ECFG-2110	2011622	EK912752	Bueno	No
11	Torre IBM		2002061	LKHPG4Y	Deficiente	Si
12	Torre IBM		2001077	LKXMA0A	Deficiente	Si
13	Torre IBM		2001732	LKXNM4H	Deficiente	Si
14	Torre IBM		2001686	LKHPH27	Deficiente	Si
15	Torre IBM		2001070	LKHPG4N	Deficiente	Si
16	Torre IBM		2001089	LKHPG1V	Deficiente	Si
17	Torre IBM		NA	LKHPH0L	Deficiente	Si
18	Torre IBM		2011659	LKHPG5	Deficiente	Si

				F	e	
19	Torre IBM		2011658	LKHPH1 L	Deficient e	Si
20	Torre IBM		2011662	NA	Deficient e	Si
21	Torre IBM		2001068	LKHPG4 P	Deficient e	Si
22	Torre IBM		NA	NA	Deficient e	Si
23	Torre IBM		2001058	LKHPG4 K	Deficient e	Si
24	100 Routers	cisco 1700	NA	NA	Bueno	No
25	Switch	ENH924-AUT	2011620	1121808 0700048	Bueno	No
26	Torre IBM		2011663	LKHPG9 M	Deficient e	Si
27	Torre IBM		2001724	LKHPG4 B	Deficient e	Si
28	Torre NEXT	NA	2009781	NA	Deficient e	Si
29	Impresora HP	C6450A	NA	MX04D1 41WN	Deficient e	Si
30	Impresora HP	C4582A	RCB-1122	SG74N1 C0XS	Deficient e	Si
31	Torre blanca	NA	NA	NA	Deficient e	Si
32	Torre Dell	DHM	NA	9W2SY0 1	Deficient e	Si
34	Torre blanca	NA	NA	NA	Deficient e	Si
35	Torre HP	XE310	2000343	MX21130 651	Deficient e	Si
36	Torre HP	XE310	2002042	MX21130 626	Deficient e	Si
37	Torre blanca	NA	NA	NA	Deficient e	Si
38	Torre blanca	NA	NA	NA	Deficient e	Si
39	Impresoras HP	C4531A	NA	SG72Q1 H17S	Deficient e	Si
40	Impresora Epson	TX105	NA	KGBZ005 334	Aceptabl e	No
41	Motor tul	RTX2A	2011577	NA	Bueno	No

42	Motor tul	RTX2A	2011559	NA	Bueno	No
43	Motor tul	RTX2A	2011594	NA	Bueno	No
44	Motor tul	RTX2A	2011596	NA	Bueno	No
45	Motor tul	RTX2A	201159	NA	Bueno	No
46	Taladro	KR750B3	2011656	NA	Bueno	No
47	Impresora HP	3820	NA	CN27111 F0V1	Deficiente	Si
48	Impresora Dell	3000	NA	NA	Deficiente	Si
49	Impresora EPSON	FX1050	ERCB-1101	0B11197 813	Deficiente	Si
50	Impresora KYOSERA	FS-1030D	NA	XPG6411 5	Deficiente	Si
51	Impresora HP	6920	NA	NA	Deficiente	Si
52	Impresora EPSON	FX1170	NA	NA	Deficiente	Si
53	Impresora EPSON	FX1170	NA	6211231 933	Deficiente	Si
54	Impresora EPSON	FX1170	NA	6211512 983	Deficiente	Si
55	Impresora HP	87DCXI	NA	US69B12 0G0	Aceptable	No
56	13 Boards variados	NA	NA	NA	Deficiente	Si
57	3 Boards variadas	NA	NA	NA	Aceptable	No
58	Teclado	SK-710	NA	NA	Deficiente	Si
59	Teclado	SK-710	NA	C960301 873	Deficiente	Si
60	Teclado HP	KB-9970	2001390	1L19802 665B	Deficiente	Si
61	Teclado HP	KB-9970	2000345	2A32601 259B	Deficiente	Si
62	Teclado Blanco	NA	NA	NA	Deficiente	Si
63	Teclado HP	KB-9970	2002047	2A32602 741B	Deficiente	Si
64	Teclado Genius	KB-10X	NA	ZM31001 51378	Deficiente	Si
65	Teclado HP	KB-9970	NA	2a32601 474b	Deficiente	Si

66	Teclado GoldStar	BTC-5349R	NA	91030508	Deficiente	Si
67	Teclado IBM	XK-8820	2001643	13876836	Deficiente	Si
68	Teclado IBM	XK-8820	2000364	NA	Deficiente	Si
69	Teclado Genius	K639	NA	ZM5239075582	Deficiente	Si
70	Teclado Genius	K639	NA	ZM5239068659	Deficiente	Si
71	Teclado IBM	XK-8820	2001734	NA	Deficiente	Si
72	Teclado IBM	XK-8820	2001067	567016	Deficiente	Si
73	Teclado IBM	XK-8820	14001	13876840	Deficiente	Si
74	Teclado IBM	XK-8820	2001712	NA	Bueno	No
75	Teclado IBM	XK-8820	2001387	200336	Bueno	No
76	Teclado Genius	K639	NA	XX8588128654	Bueno	No
77	Estabilizador Energex	PR-1500N	NA	2018392	Bueno	No
78	Estabilizador	PR 1000	NA	NA	Deficiente	Si
79	Estabilizador MEGA	NA	8714	806117	Deficiente	Si
80	Estabilizador	BC3077	2833	EW2AF	Deficiente	Si
81	Mueble	NA	2011719	NA	Deficiente	Si
82	Estabilizador	RL1000	6865	NA	Deficiente	Si
83	Sopladora MP TOOLS	NA	2011627	NA	Bueno	No
84	Sopladora MP TOOLS	NA	2002051	NA	Bueno	No
85	Sopladora MP TOOLS	NA	2011628	NA	Bueno	No
86	Sopladora MP TOOLS	NA	2011630	NA	Bueno	No
87	Taladro	TP680	2011533	NA	Bueno	No
88	Teclado IBM	SK-8820	14076	13876805	Bueno	No

89	Teclado Turbo	KB-8801	NA	NA	Deficiente	Si
90	Teclado IBM	SK-8820	2001079	638214	Deficiente	Si
91	Torre COMPUMAX	CMAX-11122CDO	NA	101SN34791	Bueno	No
92	Torre COMPUMAX	CMAX-11122CDO	NA	101SN34651	Bueno	No
93	Impresora EPSON	8750	2001565	44be058389	Deficiente	Si
94	Impresora HP	3920	NA	C9062A	Deficiente	Si
95	Impresora EPSON	8750	NA	44B1096024	Deficiente	Si
96	10 Unidades de Cd	NA	NA	NA	Deficiente	Si
97	9 Unidades de disket	NA	NA	NA	Deficiente	Si
98	Impresora HP	3535	NA	08995 ^a	Bueno	No
99	Impresora HP	3420	NA	08947 ^a	Bueno	No
100	Impresora EPSON	LX-300	NA	SP014989	Bueno	No
101	Impresora EPSON	LX-300	NA	1W6X059037	Bueno	No
102	Mouse IBM	MO28UO	NA	204696	Deficiente	Si
103	Mouse IBM	MO28UO	NA	163774	Bueno	No
104	Mouse IBM	MO28UO	1332	235998	Bueno	No
105	Mouse Genius	R31258	NA	X63308204241	Deficiente	Si
106	Mouse Genius	GM-03022P	NA	1,47085E+11	Deficiente	Si
107	Mouse HP	SBF96	NA	FB7330AN3VC1EIC	Deficiente	Si

Tabla 6. Inventario Aula 311A

LISTA DE FIGURAS

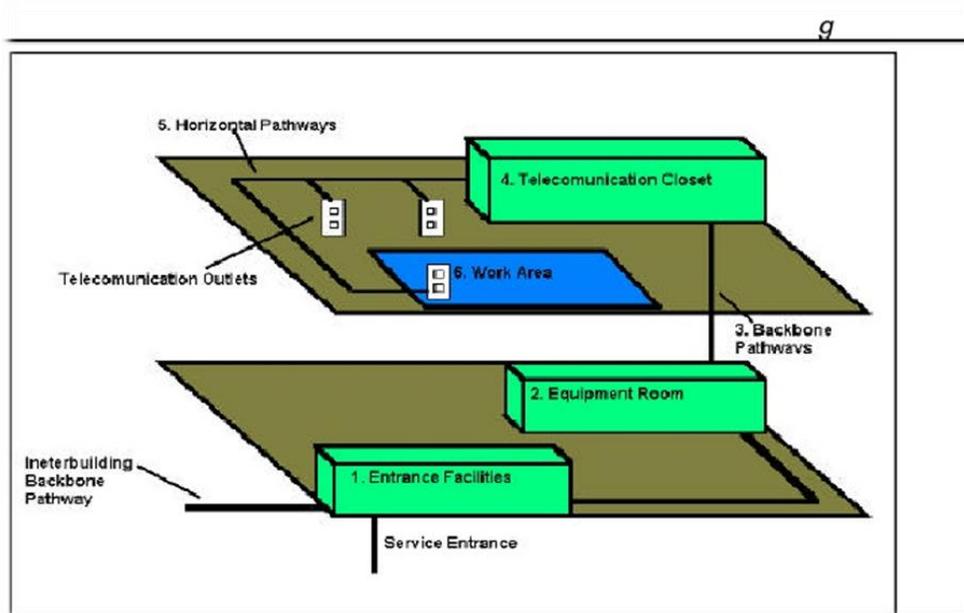


Figura1 Backbone

Número	Tema
802.1	Supervisión y arquitectura de LANs
802.2 ↓	Control lógico de enlace
802.3 *	Ethernet
802.4 ↓	Token bus (se utilizó por un corto tiempo en plantas manufactureras)
802.5	Token ring (entrada de IBM al mundo de las LANs)
802.6 ↓	Cola dual, bus dual (primera red de área metropolitana)
802.7 ↓	Grupo de consultoría técnico de tecnologías de banda ancha
802.8 †	Grupo de consultoría de tecnologías de fibra óptica
802.9 ↓	LANs síncrona (para aplicaciones de tiempo real)
802.10 ↓	LANs virtuales y seguridad
802.11 *	LANs inalámbricas
802.12 ↓	Demanda de prioridad (AnyLAN de Hewlett-Packard)
802.13	Número de mala suerte. Nadie lo quiso
802.14 ↓	Módems de cable (desaparecido: primero surgió un consorcio en la industria)
802.15 *	Redes de área personal (Bluetooth)
802.16 *	Redes inalámbricas de área ancha
802.17	Anillo de paquete elástico

Figura 2 grupos de trabajo del 802

REDES DE EJEMPLO

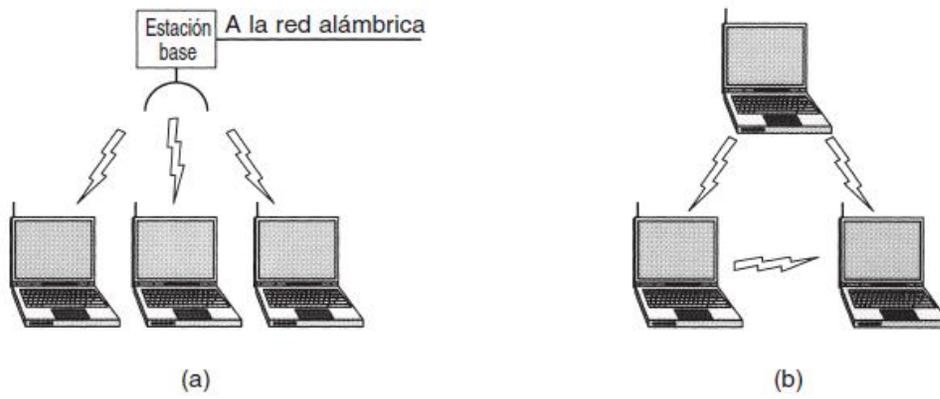


Figura 3 redes de ejemplo

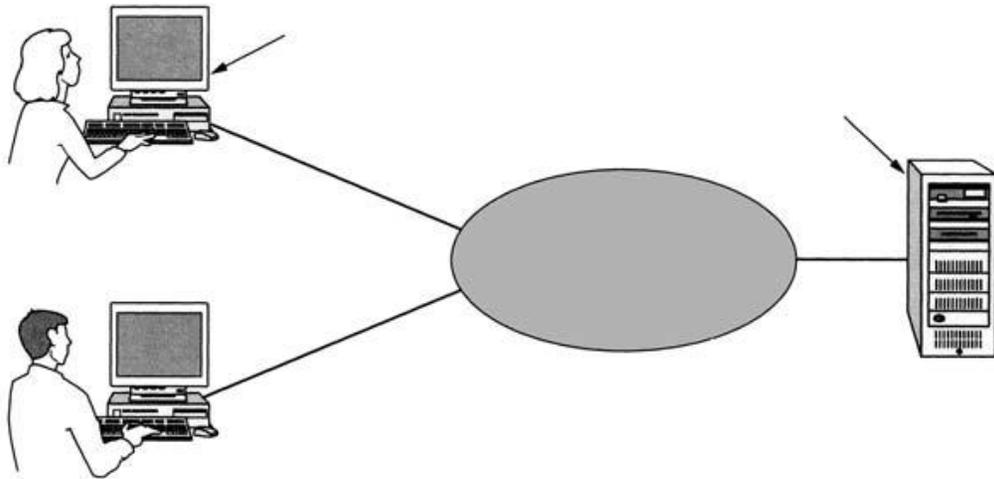


Figura 4. Una red con dos clientes y un servidor.

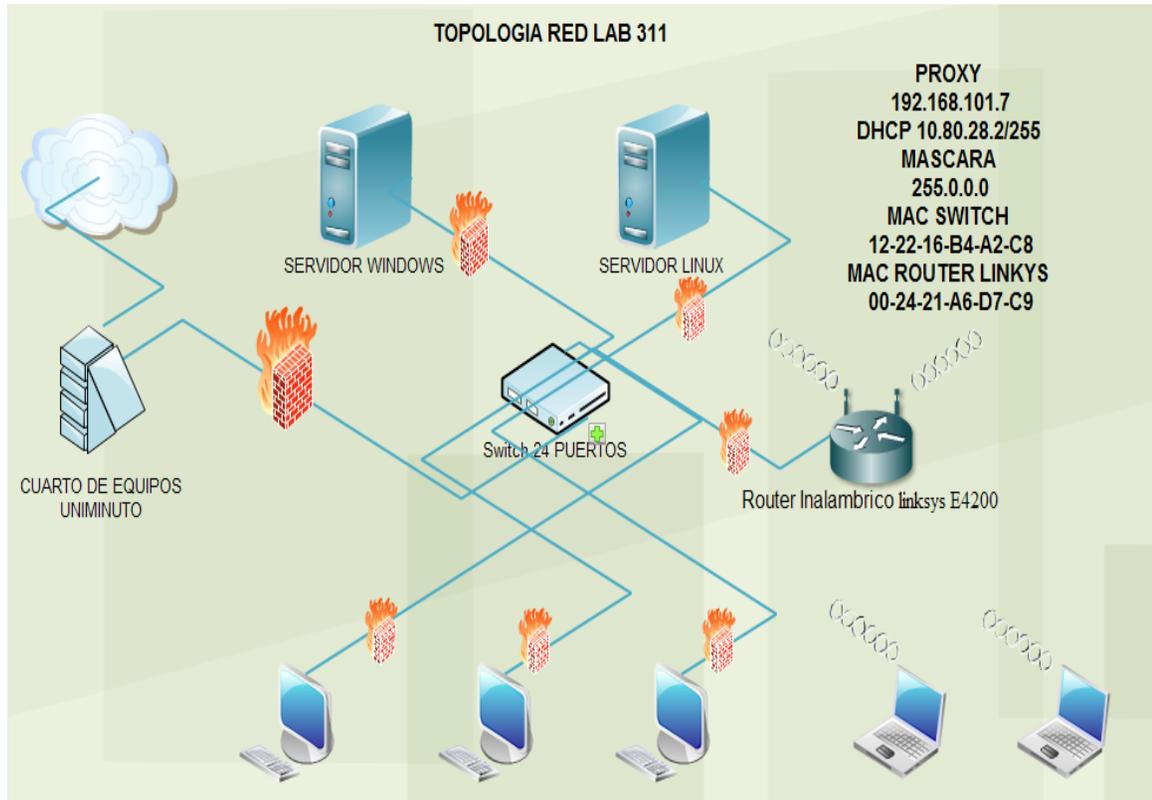


Figura 5 Topología de Red

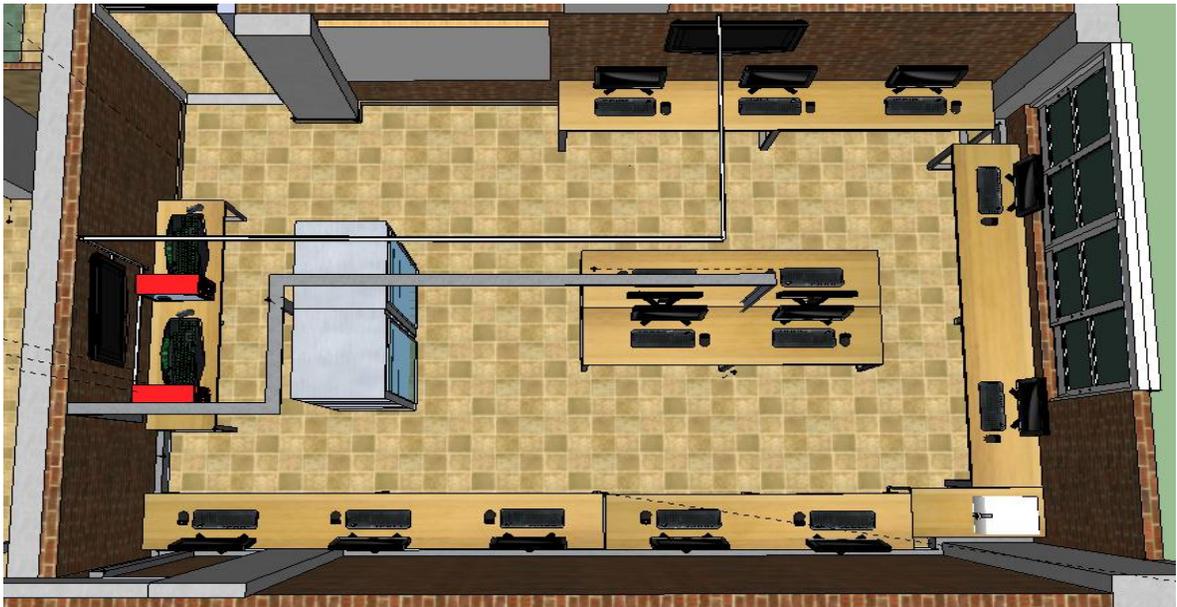


Figura 6 Laboratorio 311

7. LISTA DE ANEXOS

ANEXO I. CRONOGRAMA DE ACTIVIDADES.

Nombre de tarea	Duración	Comienzo	Fin
TESIS	177 días	mié 19/09/12	jue 23/05/13
TITULO DEL PROYECTO	1 día?	mié 19/09/12	mié 19/09/12
TEMA	1 día	mié 19/09/12	mié 19/09/12
PLANTEAMIENTO DEL	1 día?	mié 19/09/12	<u>mié 19/09/12</u>
Descripción	1 día?	jue 20/09/12	<u>jue 20/09/12</u>
Formulación Del Problema	1 día?	jue 20/09/12	<u>jue 20/09/12</u>
ALCANCES Y LIMITACIONES	6 días	lun 11/03/13	lun 18/03/13
Alcances	6 días?	lun 11/03/13	lun 18/03/13
Limitaciones	6 días?	lun 11/03/13	<u>lun 18/03/13</u>
OBJETIVOS	16 días	vie 21/09/12	<u>vie 12/10/12</u>
General	16 días?	vie 21/09/12	vie 12/10/12
Específicos	16 días?	vie 21/09/12	<u>vie 12/10/12</u>
JUSTIFICACION	5 días	mar 19/03/13	<u>lun 25/03/13</u>
MARCO DE REFERENCIA	15 días	mar 19/03/13	lun 08/04/13
Marco Historico	15 días?	mar 19/03/13	lun 08/04/13
Marco Teorico	15 días?	mar 19/03/13	<u>lun 08/04/13</u>
FASE DE INICIO	10 días	mar 09/04/13	<u>lun 22/04/13</u>
Descripción de la estructura	5 días	mar 09/04/13	lun 15/04/13
Descripción de la estructura eléctrica	5 días	mar 09/04/13	lun 15/04/13
Descripción de las zonas comunes	5 días	mar 09/04/13	lun 15/04/13
Requisitos puntos de red	27 días	mar 09/04/13	<u>mié 15/05/13</u>
Requisitos crecimiento físico de la red	10 días	mar 16/04/13	<u>lun 29/04/13</u>
Requisitos de seguridad física	10 días	mar 16/04/13	<u>lun 29/04/13</u>
Tipo de información transmitida por la red	10 días	mar 16/04/13	<u>lun 29/04/13</u>

Velocidad y flujo de datos	10 días	mar 16/04/13	<u>lun 29/04/13</u>
Requisitos de seguridad logica	10 días	mar 16/04/13	<u>lun 29/04/13</u>
▀ DISEÑO DE LA RED	10 días	mar 30/04/13	<u>lun 13/05/13</u>
Diseño fisico	5 días	mar 30/04/13	lun 06/05/13
Modulo Cableado	10 días	mar 30/04/13	<u>lun 13/05/13</u>
Modulo Inalambrico	10 días	mar 30/04/13	<u>lun 13/05/13</u>
Diseño Logico	10 días	mar 30/04/13	<u>lun 13/05/13</u>
Arquitectura de la red	10 días	mar 30/04/13	<u>lun 13/05/13</u>
Direccionamien IP	10 días	lun 06/05/13	<u>vie 17/05/13</u>
Metodos de Acceso	10 días	lun 06/05/13	<u>vie 17/05/13</u>
Metodos de Acceso	10 días	lun 06/05/13	<u>vie 17/05/13</u>
Diagrama Logico de la Red	10 días	lun 06/05/13	<u>vie 17/05/13</u>
Selección y evaluacion de tecnologias	10 días	lun 06/05/13	<u>vie 17/05/13</u>
Software	10 días	lun 06/05/13	<u>vie 17/05/13</u>
PRESUPUESTO	1 día	mié 19/09/12	mié 19/09/12
CONCLUSIONES	10 días	lun 06/05/13	vie 17/05/13
BIBLIOGRAFIAS	10 días	lun 06/05/13	vie 17/05/13
ANEXOS	15 días	lun 11/03/13	vie 29/03/13

ANEXO II. FOTOGRAFIAS ESTUDIO DE CAMPO

Centro Regional Uniminuto Cede Soacha



Ilustración 1 Salón 311 A



Ilustración 2 Salón 311 A



Ilustración 3 Salón 311^a



Ilustración 4 Salón 311A



Ilustración 5 Canaleta eléctrica y de red salón 311A



Ilustración 6 Laboratorio 311A Actual



Ilustración 7 Laboratorio 311A Actual



Ilustración 8 Laboratorio 311A Actual



Ilustración 9 Laboratorio 311A Actual



Ilustración 10 Canaleta aérea laboratorio 311A



Ilustración 11 Contadores Eléctricos CODENSA



Ilustración 12 Salida Trasera Edificio Primer Nivel



Ilustración 13 Canaleta Eléctrica Edificio



Ilustración 14 Entrada Biblioteca



Ilustración 15 Biblioteca Estudiantil



Ilustración 16 Entrada Principal Edificio



Ilustración 17 Rampa Emergencia Edificio



Ilustración 18 Costado Lateral Derecho Edificio



Ilustración 19 Costado Trasero Edificio



Ilustración 20 Costado Lateral Izquierdo Edificio



Ilustración 21 Cuarto Eléctrico Primer Nivel Edificio



Ilustración 22 Tercer Nivel Entrada Laboratorios



Ilustración 23 Escaleras Edificio



Ilustración 24 Cuarto De Equipos Tercer Nivel



Ilustración 25 Señalización Seguridad Segundo Nivel

Uniminuto Cede Calle 80



Ilustración 26 Laboratorio Redes Y Seg Inf.



Ilustración 27 Laboratorio Redes Y Seg Inf.



Ilustración 28 Cuarto de Equipos LAB Redes y Seg Inf.