ESCUELA POLITÉCNICA DEL EJÉRCITO

EXTENSIÓN - LATACUNGA

CARRERA DE TECNOLOGÍA EN COMPUTACIÓN

"DOCUMENTACIÓN DE LA RED LAN DE LOS LABORATORIOS DE REDES INFORMÁTICOS UTILIZANDO HERRAMIENTAS DE ESCANEO DE RED"

PROYECTO PREVIO LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN COMPUTACIÓN

REALIZADO POR:

SEGUNDO MANUEL ANGUISACA TRAVEZ

LUIS ROLANDO NINASUNTA GUANOQUIZA

Latacunga, Marzo del 2011

ESCUELA POLITÉCNICA DEL EJÉRCITO
EXTENSIÓN – LATACUNGA

CARRERA DE TECNOLOGÍA EN COMPUTACIÓN

AUTORIZACIÓN

Nosotros:

Cbop. Segundo Manuel Anguisaca Travez y

Cbos. Luis Rolando Ninasunta Guanoquiza

Autorizamos a la Escuela Politécnica del Ejército, la publicación en la Biblioteca virtual de la Institución, del trabajo **"DOCUMENTACIÓN DE LA RED LAN DE LOS LABORATORIOS DE REDES INFORMÁTICOS UTILIZANDO HERRAMIENTAS DE ESCANEO DE RED "**, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Latacunga, marzo 2011

Cbop. Segundo Anguisaca	Cbos. Luis Ninasunta
C.I. 0502625718	C.I. 0502746233

ESCUELA POLITÉCNICA DEL EJÉRCITO
EXTENSIÓN - LATACUNGA

CARRERA DE TECNOLOGÍA EN COMPUTACIÓN

DECLARACIÓN DE RESPONSABILIDAD

Nosotros:

Cbop. Segundo Manuel Anguisaca Travez y
Cbos. Luis Rolando Ninasunta Guanoquiza

DECLARAMOS QUE:

El proyecto de grado denominado: **"DOCUMENTACIÓN DE LA RED LAN DE LOS LABORATORIOS DE REDES INFORMÁTICOS UTILIZANDO HERRAMIENTAS DE ESCANEO DE RED "** ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de nuestra autoría.

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

Latacunga, marzo del 2011

Cbop. Segundo Anguisaca	Cbos. Luis Ninasunta
C.I. 0502625718	C.I. 0502746233

ESCUELA POLITÉCNICA DEL EJÉRCITO
EXTENSIÓN - LATACUNGA

CARRERA DE TECNOLOGÍA EN COMPUTACIÓN

CERTIFICADO

ING. César Naranjo (Director)

ING. Mayra Salazar (Codirector)

CERTIFICAN:

Que el trabajo titulado **"DOCUMENTACIÓN DE LA RED LAN DE LOS LABORATORIOS DE REDES INFORMÁTICOS UTILIZANDO HERRAMIENTAS DE ESCANEO DE RED "**, realizado por los señores: Cbop. Segundo Manuel Anguisaca Travez y el Sr. Cbos. Luis Rolando Ninasunta Guanoquiza, ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Escuela Politécnica del Ejército.

Debido a que constituye un trabajo de excelente contenido científico que coadyuvará a la aplicación de conocimientos y al desarrollo profesional, **SI** recomiendan su publicación.

El mencionado trabajo consta de UN empastado y UN disco compacto el cual contiene los archivos en formato portátil de Acrobat. Autorizan a los señores: Cbop. Segundo Manuel Anguisaca Travez y el Cbos. Luis Rolando Ninasunta Guanoquiza, que lo entregue al ING. José Luis Carrillo, en su calidad de Director de Carrera.

Latacunga, marzo de 2011.

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

Ing. César Naranjo — **DIRECTOR**

Ing. Mayra Salazar — **CODIRECTOR**

AGRADECIMIENTO

Primero antes que nada mi agradecimiento especial a Dios, por darme la vida, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente, por haberme dado unos excelentes padres y una linda familia, por haberme puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante el periodo de formación profesional.

Agradezco hoy y siempre a mi familia porque a pesar de no estar presente físicamente han estado conmigo cada día dándome animo y la fortaleza necesaria para seguir adelante.

Agradezco a la Escuela Politécnica del Ejercito Extensión Latacunga, ya que me abrió sus puertas para poder formarme profesional e intelectualmente.

A la carrera de Sistemas e Informática a sus profesores, por todos los conocimientos que me brindaron.

Agradezco al director de este proyecto Ingeniero Cesar Naranjo y codirectora Ingeniera Mayra Salazar por su apoyo, confianza y apertura para poder culminar con éxito el presente proyecto.

Un profundo agradecimiento a las personas que trabajan en el Departamento de los Laboratorios de Redes Informáticos, por su apoyo y sus conocimientos en todo momento que requería sin ningún egoísmo, gracias por todo.

LUIS R. NINASUNTA G.

DEDICATORIA

Quiero dedicar este trabajo a Dios, por su grande misericordia y amor que me permitido culminar este trabajo.

Dedico este trabajo con todo el amor del mundo a mis padres Rafael y Francisca que les amo mucho, por escucharme, por sus sabios concejos, por enseñarme a luchar, por su amor quienes me ayudan a encontrar la luz cuando todo es oscuridad, por su apoyo moral y económicamente, y por estar siempre a mi lado en los momentos difíciles que Dios le bendiga, les proteja siempre y les de muchos años de vida.

A quienes un día les prometí que terminaría mis estudios, hoy mi triunfo es el de usted queridos padres los ¡Amo...!

A mi esposa, Miriam Castro, quien me brindo su amor, su cariño, su estimulo, su comprensión, su paciencia y su apoyo constante en todo momento.

A mi hijo Jonathan y mi hija Katherine quienes me presentaron el tiempo que le pertenecía ¡Gracias, mis amores!, sin ustedes no hubiese podido hacer realidad este sueño.

A los que nunca dudaron que lograría este triunfo: mi querida familia mis abuelos(a), mis hermanos, mi hermana, mis tíos(as), mis primos(as), mis sobrinos(as) y mis cuñados(as).

LUIS R. NINASUNTA G.

DEDICATORIA

En la vida hay personas muy importantes, que siempre te brindan apoyo, te extienden la mano en momentos difíciles, te escuchan, por todo eso, dedico este trabajo con todo el amor del mundo a mi familia que les admiro y les amo mucho, gracias por todo lo que han hecho por mí, por el apoyo que me han brindado tanto moral como económicamente, que Dios le bendiga y les proteja siempre.

A mi esposa, Dolores Cofre, quien me brindó su amor, su cariño, su estímulo y su apoyo constante. Su cariño, comprensión y paciente espera para que pudiera terminar el grado son evidencia de su gran amor.

A mi adorada hija Denisse Mabel quien me prestó el tiempo que le pertenecía para terminar y me motivó siempre con sus caricias, ternura y pasión, Gracias, mi bella princesa.

A mis padres, Carlos y María quienes me enseñaron desde pequeño a luchar para alcanzar mis metas. Mi triunfo es el de ustedes, "gracias"

A los que nunca dudaron que lograría este triunfo: mi hermana Ercelinda y mí cuñado Ricardo, mis hermanas, hermanos y cuñados, quien siempre me motivó a seguir adelante y a quien prometí que terminaría mis estudios. Promesa cumplida.

SEGUNDO M. ANGUISACA T.

ÍNDICE DE CONTENIDOS

CAPÍTULO 1

GENERALIDADES

CAPITULO 2

EL PROBLEMA

CONTENIDO **Pág.**

CAPÍTULO 3
ANÁLISIS Y PROCEDIMIENTOS DE LA INVESTIGACIÓN

CONTENIDO **Pág.**

CAPÍTULO 4

ELABORACIÓN DEL MANUAL Y PRESENTACIÓN DE RESULTADOS

CONTENIDO **Pág.**

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

INDICE DE FIGURAS

INDICE DE TABLAS

CONTENIDO **Pág.**

RESUMEN

El nuevo paradigma que rige actualmente en las Instituciones es la automatización y digitalización de sus procesos de trabajo, de manera que se adapten a las necesidades de las mismas, con la finalidad de generar recursos que le permita posicionarse en el entorno globalizado y tomar decisiones con menor grado de incertidumbre ante los diversos eventos presentados en los escenarios actuales. Por ello, el presente trabajo de investigación mediante las tecnologías de información utilizando herramientas de gran capacidad como (GFI Languard Scanner) que sirve de soporte para el proceso de escaneo de la red (LAN). Para ello, se requiere manejar las tecnologías en forma apropiada, los cuales se traducen finalmente en una administración de conocimiento organizacional, fundamentado en el manejo de la información en forma apropiada.

Las redes informáticas son sistemas que permiten conectar ordenadores y otros equipos informáticos entre sí, con la finalidad de compartir información y recursos, esto permite que la comunicación no sea muy complicada entre diferentes usuarios que estén conectados a la red en la Institución que opte por tener una red informática. Mediante el proceso de compartir información y recursos en una red, los usuarios de los diferentes sistemas informáticos de la organización a la que pertenece podrán hacer un mejor uso de los mismos, mejorando de este modo el rendimiento global de la organización. Para visualizar de mejor forma lo referente al escaneo de redes, vamos a citar varias de las ventajas:

- Mayor facilidad en la comunicación entre usuarios
- Reducción problemas en la red
- Mejoras en la administración de los equipos y programas
- Mayor seguridad para acceder a la información

INTRODUCCIÓN

Con el avance de la tecnología de punta y la facilidad que nos brinda el Internet de obtener información y en respuesta a las necesidades del Departamento de Eléctrica e Electrónica en especial la carrera de Tecnología en Computación, que ha propuesto elaborar un manual de monitoreo y escaneo de todo los puntos de red instalados en los laboratorios informáticos, esto se constituirá en una ayuda muy importante para el personal que trabaja en ella.

El levantamiento de la información facilitará de gran manera a encontrar y solucionar los posibles inconvenientes o errores en los puntos o elementos activos de una red.

La meta principal de la ESPE Extensión Latacunga es ofrecer soluciones simples y confiables a sus necesidades en base a trabajos sujetas a normas y estándares de calidad.

El trabajo de investigación se presenta en V capítulos. El capítulo I. Los objetivos de la investigación, la fundamentación teórica, estándares y dispositivos de red.

El Capitulo II, encuentra el desarrollo de los antecedentes investigativos que apoyan este estudio, el planteamiento del Problema, la situación actual, la justificación de la investigación y los métodos de supervisión de redes.

El Capítulo III, se realiza la determinación de los requerimientos, análisis de diseño de Solución de Seguridad y la Instalación de LANguard Network Security Scanner que se empleara en el estudio.

El Capítulo IV, indicamos la elaboración del manual, y la presentación de resultados obtenidos en la investigación y se presenta el diagnóstico y análisis de la situación actual.

En el capitulo V, se indican las conclusiones y las recomendaciones finales obtenidas de la presente investigación desarrollada en la Escuela Politécnica del Ejército Extensión Latacunga con la colaboración del cuerpo docente.

CAPÍTULO 1

GENERALIDADES

1.1 OBJETIVOS DE LA INVESTIVACIÓN:

OBJETIVOS GENERAL:

Realizar la documentación de La red LAN de los Laboratorios de Redes Informáticos utilizando herramientas de escaneo de red.

OBJETIVOS ESPECÍFICO:

- Escanear la red utilizando una herramienta para solucionar problemas en el menor tiempo y con seguridad
- Verificar el nivel de tráfico existente en la red de área local de los laboratorios informáticos a través del escaneo.
- Describir las características de cada uno de los equipos instalados en los laboratorios para tener un mejor control.
- Diseñar un plano con los puntos principales de la red.
- Desarrollar un manual de ayuda para el administrador y usuarios.

1.2 FUNDAMENTACIÓN TEÓRICA

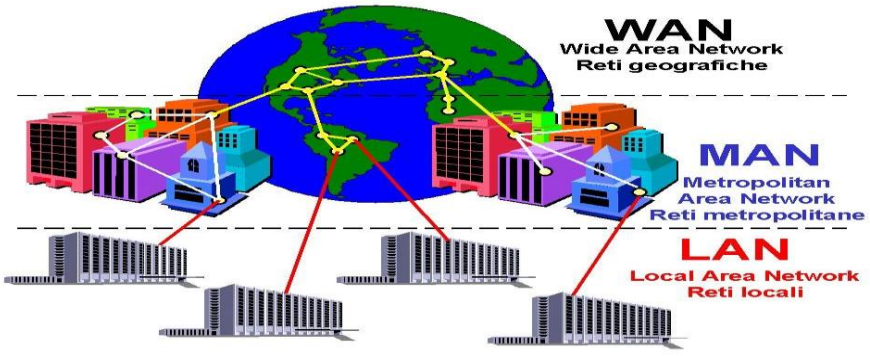


Figura 1.1. Diagrama de una red.

Al conjunto de computadoras, equipos de comunicación y otros dispositivos que se pueden comunicar entre si, a través de un medio en particular se afina red. (Ver Figura 1.1)

Las caracterizas básicas que deben cumplir las arquitecturas de red son:

1. **Tolerancia a fallas.-** limita el impacto de una falla del software o hardware
2. **Escalabilidad.-** puede expandirse rápidamente para admitir a nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio.
3. **Calidad del servicio.-** La calidad de estos servicios se miden con la calidad de experimentar la misma presentación de audio y video en personas.
4. **Seguridad.-** la rápida expansión de las redes de comunicación aumenta la necesidad de incorporar seguridad en la arquitectura.

1.2.1 RED LAN

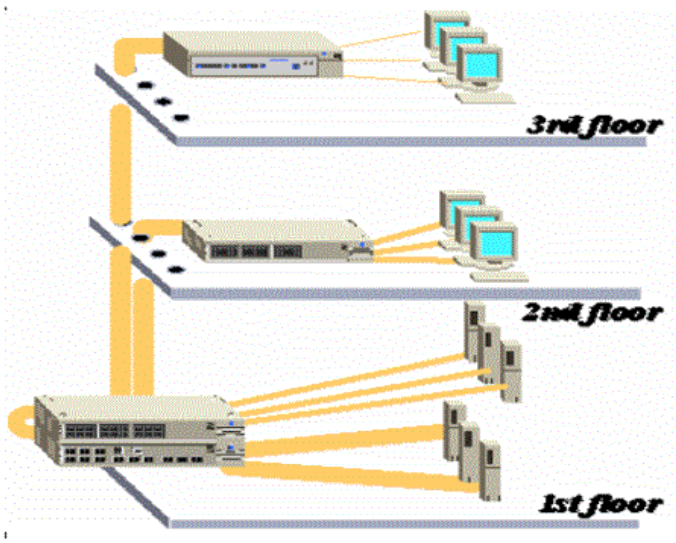


Figura 1.2 Red LAN

LAN es la abreviatura de Local Área Network (Red de Área Local).

Una red de área local es la interconexión de varios ordenadores y periféricos para intercambiar recursos e información. En definitiva, permite que dos o más máquinas se comuniquen. (Ver Figura 1.2)

Una red de área local es un sistema de transmisión de datos que permite que la comunicación entre diferentes dispositivos de tratamientos de datos.

Los inicios experimentales de la red de área local se dan desde la década de los sesenta hasta la mitad de los setenta. Fueron importantes los trabajos realizados por Bell Telephone Laboratories en redes con topología en anillo, en Xerox Corporation donde se desarrolló la primera Ethernet.

La segunda etapa, data de los finales de los setenta. Coincide con el incremento de las prestaciones y con los primeros productos en el mercado. Empieza a aparecer numerosas empresas con servicios de redes locales.

La última etapa se inicia a principios de los ochenta cuando el IEEE 802 empieza a influir en lo relacionado con las redes locales. Se afianza las topologías en anillo y en bus. Prosperan los protocolos basados en CSMA/CD. (Siglas que corresponden a **Carrier Sense Multiple Access with Collision Detection** (en español, "**Acceso Múltiple por Detección de Portadora con Detección de Colisiones**"), es una técnica usada en redes Ethernet para mejorar sus prestaciones. Anteriormente a esta técnica se usaron las de Aloha puro y Aloha ranurado, pero ambas presentaban muy bajas prestaciones. Por eso apareció en primer lugar la técnica CSMA, que fue posteriormente mejorada con la aparición de CSMA/CD.) Todos los dispositivos pueden comunicarse con el resto aunque también pueden funcionar de forma independiente. Las velocidades de comunicación son elevadas estando en el orden de varios millones de bits por segundo dependiendo del tipo de red que se use.

Características de LAN:

- Capacidad de transmisión comprendida entre 1 Mbps y 1 Gbps.
- Extensión máxima no superior a 3 km (una FDDI[1] puede llegar a 200 km).
- Uso de un medio de comunicación privado.
- La facilidad con que se pueden efectuar cambios en el hardware y el software.
- Gran variedad y número de dispositivos conectados.
- Posibilidad de conexión con otras redes.
- Limitante de 100 m, puede llegar a más si se usan repetidores.

1.2.2 RED MAN[2]

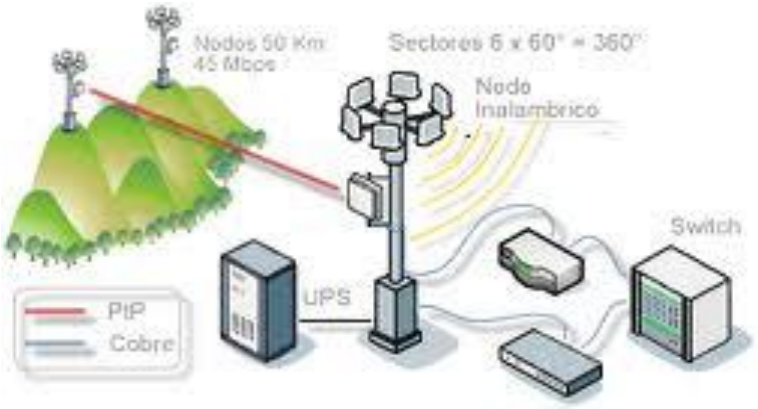


Figura 1.3 Red MAN.

Es una versión más grande de una LAN en cuanto a topología, protocolos y medios de trasmisión, que interconectan redes de área local (LAN) por ejemplo puede cubrir un conjunto de oficinas corporativas o empresas en una ciudad. Cualquier red de datos, voz o video con una extensión de una o varios decenas de kilómetros puede ser considerada una MAN. (Ver Figura 1.3)

---

[1] (FDDI.- Interfaz de distribución de datos de fibra óptica)
http://www.google.com.ec/images?hl=es&source=imghp&biw=1167&bih=465&q=redes&gbv=2&aq=f&aqi=g10&aql=&oq=&gs_rfai=

Características de la MAN[3]:

1. Se caracterizan por utilizar normalmente medios telefónicos, diseñados en principio para transportar la voz.
2. Son servicios contratados normalmente a operadoras (telefónicas)
3. Las comunicaciones tiene un costo elevado, por lo que se suele optimizar su diseño.
4. Normalmente utilizan enlaces punto a punto temporal o permanente.
5. Permiten alcanzar un diámetro entorno a los 50 kms, dependiendo el alcance entre nodos de red y de tipo de cables utilizados.

1.2.3 RED WAN

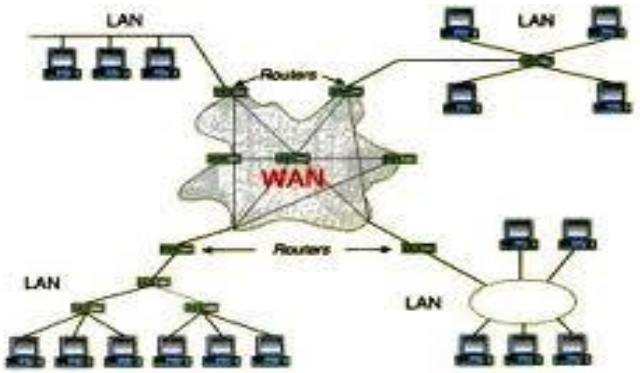


Figura 1.4 Red WAN.

Son redes que se expanden en una gran zona geográfica, por ejemplo un país o Continente. A la infraestructura que une los nodos de usuarios finales se les llama subred y abarca diversos dispositivos de red (llamado Routers o Ruteadores) y línea de comunicación que unen las diversas redes. (Ver Figura 1.4)

Características de la WAN:

[3]http://es.kioskea.net/contents/technologies/ethernet.php3

1. Conectan dispositivos que están separados por áreas geográficas extensas.
2. Utilizan los servicios de proveedores de telecomunicaciones.
3. Usan conexiones seriales de diversos tipos para acceder al ancho de banda a través de áreas geográficas extensas.

1.3 TOPOLOGÍA DE RED

La topología de red se refiere a la forma en que están interconectados los distintos equipos (Nodos) de una red. Un nodo es un dispositivo activo conectado a la red, como un computador o una impresora.

Por ejemplo, la topología de red que se utiliza en la Escuela Politécnica de Ejército Extensión Latacunga es la topología de estrella, esta topología en redes LAN hace referencia que cada estación esta directamente conectada a un nodo central, generalmente a través de dos enlaces punto a punto, uno para transmisión y otro para recepción.

Entre las ventajas de utilizar la topología estrella se tiene las siguientes:

- Todas las estaciones de trabajo están conectadas a un punto central (Concentrador), formando una estrella física.
- Cada vez que se quiere establecer comunicación entre dos ordenadores, la información transferida de uno hacia el otro debe pasar por el punto central.
- Si se rompe un cable sólo se pierde la conexión del nodo que lo interconecta.
- Es más accesible detectar y de localizar un problema en la red.

Dependiendo de la topología será la distribución física de la red y dispositivos conectados a la misma, así como también las características de ciertos aspectos de la red como: velocidad de transmisión de datos y confiabilidad del conexionado.

a. TOPOLOGÍA FÍSICAS: Es la forma que adopta un plano esquemático del cableado o estructura física de la red, también se habla de métodos de control.

b. TOPOLOGÍA LÓGICAS: Es la forma de cómo la red reconoce a cada conexión de estación de trabajo. Estos se clasifican en:

1.3.1 TOPOLOGÍA LINEAL O BUS

Consiste en un solo cable al cual se le conectan todas las estaciones de trabajo.

En este sistema una sola computadora por vez puede mandar datos los cuales son escuchados por todas las computadoras que integran el bus, pero solo el receptor designado los utiliza.

Ventajas:

- Es la más barata, apta para oficinas medianas y chicas.

Desventajas:

- Si se tienen demasiadas computadoras conectadas a la vez, la eficiencia baja notablemente.
- Es posible que dos computadoras intenten transmitir al mismo tiempo provocando lo que se denomina "colisión", y por lo tanto se produce un reintento de transmisión.
- Un corte en cualquier punto del cable interrumpe la red
- El ancho de banda varía según el tipo de medio, además de las tecnologías LAN y WAN utilizadas. La física de los medios fundamenta algunas de las diferencias.
- Las señales se transmiten a través de cables de cobre de par trenzado, coaxiales, fibras ópticas, y por el aire. Las diferencias físicas en las formas en que se transmiten las señales son las que generan las limitaciones fundamentales en la capacidad que posee un medio dado

para transportar información. No obstante, el verdadero ancho de banda de una red queda determinado por una combinación de los medios físicos y las tecnologías seleccionadas para señalizar y detectar señales de red. (Ver Figura 1.5)

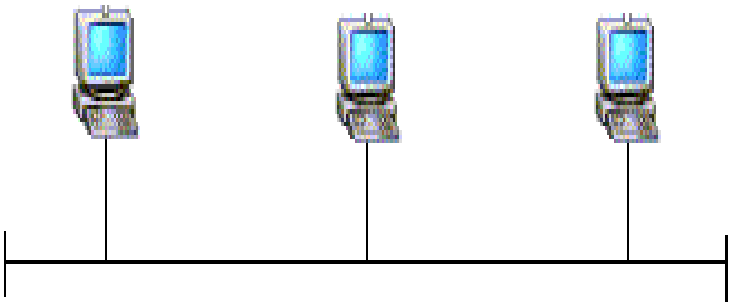


Figura 1.5 Topología Lineal.

1.3.2 TOPOLOGÍA ESTRELLA

En este esquema todas las estaciones están conectadas a un concentrador o HUB con cable por computadora. Para futuras ampliaciones pueden colocarse otros HUBs en cascada dando lugar a la estrella jerárquica.

Por ejemplo en la estructura CLIENTE-SERVIDOR: el servidor está conectado al HUB activo, de este a los pasivos y finalmente a las estaciones de trabajo. (Ver Figura 1.6)

Ventajas:

- La ausencia de colisiones en la transmisión y dialogo directo de cada estación con el servidor.
- La caída de una estación no anula la red.

Desventajas:

- Baja transmisión de datos.

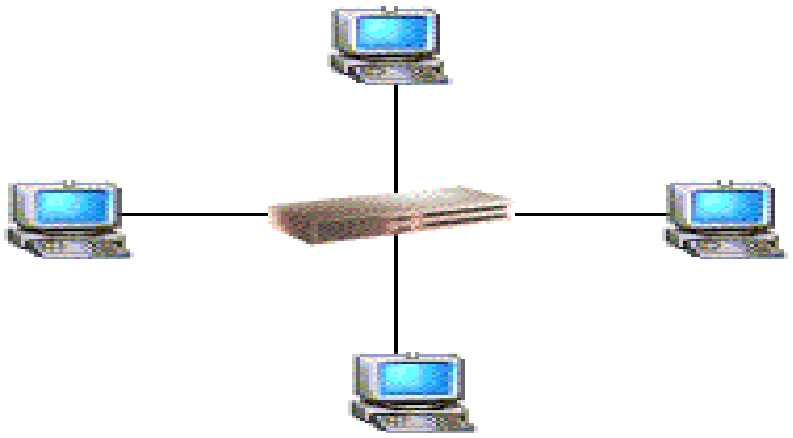


Figura 1.6 Topología Estrella.

1.3.3 TOPOLOGÍA ANILLO (TOKEN RING)

"Token Ring" es el término utilizado para referirse a la norma IEEE 802.5 para implementar una red LAN con topología lógica de anillo. Tecnología creada originalmente por IBM (algunos la llaman "IBM Token Ring"). (Ver Figura 1.7)

Los servidores pueden estar en cualquier lugar del anillo y la información es pasada en un único sentido de una a otra estación hasta que alcanza su destino. Cada estación que recibe el TOKEN regenera la señal y la transmite a la siguiente.

Por ejemplo en esta topología, envía una señal por toda la red. Si la terminal quiere transmitir pide el TOKEN, hasta que lo tiene puede transmitir. Si no está la señal la pasa a la siguiente en el anillo y sigue circulando hasta que alguna pide permiso para transmitir.

Ventajas:

- No existen colisiones, Pues cada paquete tienen una cabecera o TOKEN que identifica al destino.

Desventajas:

- La caída de una estación interrumpe toda la red. Actualmente no hay conexiones físicas entre estaciones, sino que existen centrales de cableado o MAU[4] que implementa la lógica de anillo sin que estén conectadas entre sí evitando las caídas.
- Es costosa, llegando a costar una placa de red lo que una estación de trabajo.

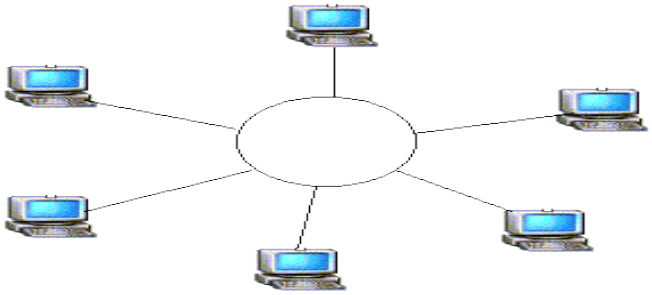


Figura 1.7 Topología en anillo.

1.3.4 TOPOLOGÍA ÁRBOL

En esta topología que es una generalización del tipo bus, el árbol tiene su primer nodo en la raíz y se expande hacia fuera utilizando ramas, en donde se conectan las demás terminales. (Figura 1.8). Esta topología permite que la red se expanda y al mismo tiempo asegura que nada más existe una ruta de datos entre dos terminales cualesquiera.

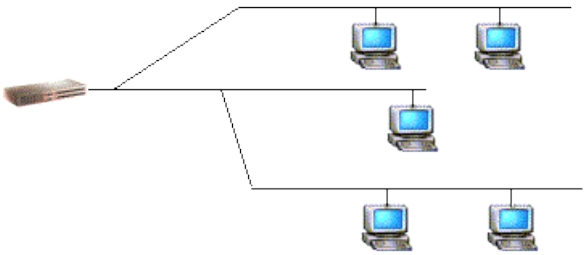


Figura 1.8 Topología Árbol

[4] MAU: Medio de unidad de acceso

1.3.5 TOPOLOGÍA MESH

Este tipo de topología es común en lugares en donde sí tenían una red bus y luego la fueron expandiendo en estrella. Son complicadas para detectar su conexión por parte del servicio técnico para su reparación. (Ver Figura 1.9)

MAU (Medio de unidad de acceso). Cada computadora necesita el "hardware" para transmitir y recibir información

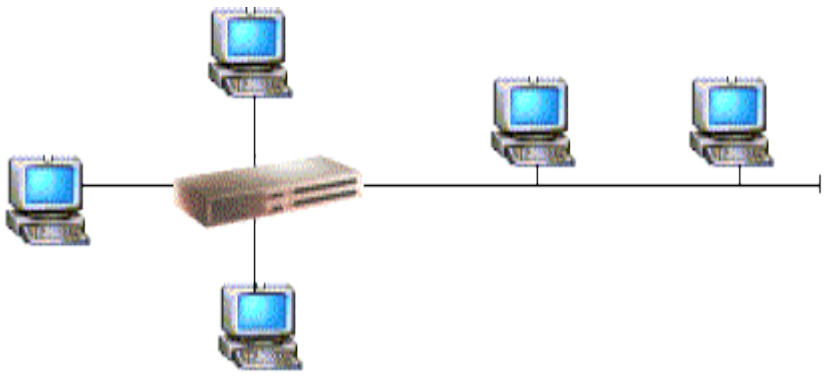


Figura 1.9 Topología Mesh

Dentro de estas topologías se tiene:

a. TOPOLOGÍA ANILLO EN ESTRELLA: se utilizan con el fin de facilitar la administración de la red. Físicamente la red es una estrella centralizada en un concentrador o HUBs, mientras que a nivel lógico la red es un anillo.

b. TOPOLOGÍA BUS EN ESTRELLA: el fin es igual al anterior. En este caso la red es un bus que se cablea físicamente como una estrella mediante el uso de concentradores.

c. TOPOLOGÍA ESTRELLA JERÁRQUICA: esta estructura se utiliza en la mayor parte de las redes locales actuales. Por medio de concentradores dispuestos en cascadas para formar una red jerárquica.

Colisión: Situación que ocurre cuando dos o más dispositivos intentan enviar una señal a través de un mismo canal al mismo tiempo

1.4 DISPOSITIVOS DE LA RED[5]

1.4.1 NIC/MAU (Tarjeta de red)

"Network Interface Card" (Tarjeta de interfaz de red). Cada computadora necesita el "hardware" para transmitir y recibir información. Es el dispositivo que conecta la computadora u otro equipo de red con el medio físico. La NIC es un tipo de tarjeta de expansión de la computadora y proporciona un puerto en la parte posterior de la PC al cual se conecta el cable de la red. Hoy en día cada vez son más los equipos que disponen de interfaz de red, principalmente Ethernet, incorporadas. A veces, es necesario, además de la tarjeta de red, un transceptor. Este es un dispositivo que se conecta al medio físico y a la tarjeta, bien porque no sea posible la conexión directa (10 base 5) o porque el medio sea distinto del que utiliza la tarjeta. (Ver Figura 1.10)

Figura 1.10 Tarjeta de red

[5] http://www.monografias.com/trabajos30/redes-de-datos/redes-de-datos.shtml
http://www.ordenadores-y-portatiles.com/wimax.html

1.4.2 Hubs (Concentradores)

Son equipos que permiten estructurar el cableado de las redes. La variedad de tipos y características de estos equipos es muy grande. En un principio eran solo concentradores de cableado, pero cada vez disponen de mayor número de capacidad de la red, gestión remota, etc. La tendencia es a incorporar más funciones en el concentrador. Existen concentradores para todo tipo de medios físicos. (Ver Figura 1.11)

Figura 1.11 Hubs

1.4.3 Repetidores

Son equipos que actúan a nivel físico. Prolongan la longitud de la red uniendo dos segmentos y amplificando la señal, pero junto con ella amplifican también el ruido. La red sigue siendo una sola, con lo cual, siguen siendo válidas las limitaciones en cuanto al número de estaciones que pueden compartir el medio. (Ver Figura 1.12). Se establecen dos tipos de repetidores: Los denominados interurbanos o de amplia cobertura y los urbanos o de cobertura restringida.

1. Repetidores interurbanos: Son aquellos que, instalados en los lugares dominantes, dan servicio a colectivos de aficionados dispersos en grandes áreas.

2. Repetidores urbanos: Son aquellos que, situados en el casco urbano, dan servicio a colectivos de aficionados existentes en la localidad y que

carecen de capacidad de efectuar contacto entre sí, particularmente a estaciones móviles y portátiles.

Figura 1.12 Repetidores

1.4.4 "Bridges" (Puentes)

Son equipos que unen dos redes actuando sobre los protocolos de bajo nivel, en el nivel de control de acceso al medio. Solo el tráfico de una red que va dirigido a la otra atraviesa el dispositivo. Esto permite a los administradores dividir las redes en segmentos lógicos, descargando de tráfico las interconexiones. Los bridges producen las señales, con lo cual no se transmite ruido a través de ellos. (Ver Figura 1.13)

Figura 1.13 Bridges

1.4.5 Switch

El switch (palabra que significa “conmutador”) es un dispositivo que permite la interconexión de redes sólo cuando esta conexión es necesaria. Para entender mejor que es lo que realiza, pensemos que la red está dividida en segmentos por lo que, cuando alguien envía un mensaje desde

un segmento hacia otro segmento determinado, el switch se encargará de hacer que ese mensaje llegue única y exclusivamente al segmento requerido. (Ver Fig. 1.14)

Figura 1.14 Switches

1.4.6 "Routers" (Encaminadores)

Son equipos de interconexión de redes que actúan a nivel de los protocolos de red. Permite utilizar varios sistemas de interconexión mejorando el rendimiento de la transmisión entre redes. Su funcionamiento es más lento que los bridges pero su capacidad es mayor. Permiten, incluso, enlazar dos redes basadas en un protocolo, por medio de otra que utilice un protocolo diferente. (Ver Figura 1.15)

Figura 1.15 Routers

1.4.7 "Gateway"

Son equipos para interconectar redes con protocolos y arquitecturas completamente diferentes a todos los niveles de comunicación. La traducción de las unidades de información reduce mucho la velocidad de transmisión a través de estos equipos. (Ver Figura 1.16)

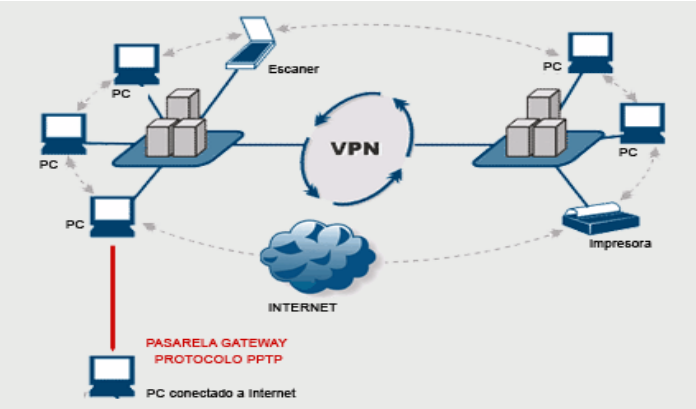


Figura 1.16 Gateway

1.4.8 Servidores

Son equipos que permiten la conexión a la red de equipos periféricos tanto para la entrada como para la salida de datos. Estos dispositivos se ofrecen en la red como recursos compartidos. Así un terminal conectado a uno de estos dispositivos puede establecer sesiones contra varios ordenadores multiusuario disponibles en la red. Igualmente, cualquier sistema de la red puede imprimir en las impresoras conectadas a un servidor. (Ver Figura 1.17)

Figura 1.17 Servidores

1.4.9 Módems

Son equipos que permiten a las computadoras comunicarse entre sí a través de líneas telefónicas; modulación y demodulación de señales electrónicas que pueden ser procesadas por computadoras. Los módems pueden ser externos (un dispositivo de comunicación) o interno

(dispositivo de comunicación interno o tarjeta de circuitos que se inserta en una de las ranuras de expansión de la computadora). (Ver Figura 1.18)

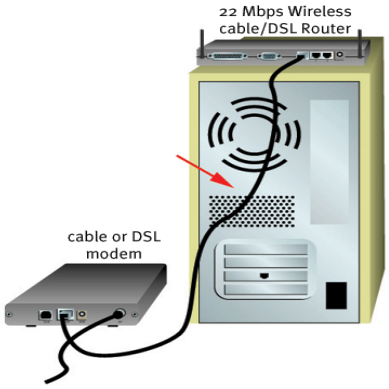


Figura 1.18 Módems

1.5 ESTANDARES DE RED

Los estándares son desarrollados por organismos reconocidos internacionalmente, tal es el caso de la IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) y la ETSI (European Telecomunications Standards Institute). Una vez desarrollados se convierten en la base de los fabricantes para desarrollar sus productos. Estándares (normas) y compatibilidad. La cuestión más importante en el campo informático. Como industria no regulada, se ha llegado a tener miles de formatos de datos y lenguajes, pero muy pocos estándares que se empleen universalmente. Sin importar lo mucho que se hable en la industria acerca de compatibilidad, aparecen rutinariamente nuevos formatos y lenguajes.

Si un formato o lenguaje se usa extensamente y otros lo copian, se convierte en un estándar de hecho y puede pasar a ser usado tan ampliamente como los estándares oficiales creados por organizaciones tales como:

- ISO International Standards Organization (Organización Internacional de Normas)
- IEEE (Instituto de ingenieros electrónicos y eléctricos) Es la encargada de fijar los estándares de los elementos físicos de una red, cables, conectores, etc.
- El comité que se ocupa de los estándares de computadoras a nivel mundial es de la IEEE en su división 802, los cuales se dedican a lo referente de sistema de red. Este tiene su propia clasificación:
- IEEE 802.3: Hace referencia a las redes tipo bus en donde se deben de evitar las colisiones de paquetes de información, por lo cual este estándar hace regencia el uso de CSMA/CD (Acceso múltiple con detención de portadora con detención de colisión)
- IEEE 802.4: Hace referencia al método de acceso Token pero para una red con topología en anillo o la conocida como token bus.
- IEEE 802.5: Hace referencia al método de acceso token, pero para una red con topología en anillo, conocida como la toquen ring.

CSMA/CD.- "Acceso Múltiple por Detección de Portadora con Detección de Colisiones"), es una técnica usada en redes Ethernet para mejorar sus prestaciones.

En el método de acceso CSMA/CD, los dispositivos de red que tienen datos para transmitir funcionan en el modo "escuchar antes de transmitir". Esto significa que cuando un nodo desea enviar datos, primero debe determinar si los medios de red están ocupados o no.

TOKEN BUS.- Es un protocolo de acceso al medio en el cual los nodos están conectados a un bus o canal para comunicarse con el resto. En todo momento hay un testigo (token) que los nodos de la red se van pasando, y únicamente el nodo que tiene el testigo tiene permiso para transmitir. El bus principal consiste en un cable coaxial.

1.5.1 ESTANDAR ETHERNET[6]

Ethernet (también conocido como estándar IEEE 802.3) es un estándar de transmisión de datos para redes de área local que se basa en el siguiente principio:

Todos los equipos en una red Ethernet están conectados a la misma línea de comunicación compuesta por cables cilíndricos. Se distinguen diferentes tecnologías Ethernet según el tipo y el diámetro de los cables utilizados:

- **10Base2:** el cable que se usa es un cable coaxial delgado, llamado thin Ethernet.
- **10Base5:** el cable que se usa es un cable coaxial grueso, llamado thick Ethernet.
- **10Base-T:** se utilizan dos cables trenzados (la T significa twisted pair) y alcanza una velocidad de 10 Mbps.
- **100Base-FX**: permite alcanzar una velocidad de 100 Mbps al usar una fibra óptica multimodo (la F es por *Fiber*).
- **1000Base-T**: utiliza dos pares de cables trenzados de categoría 5 y permite una velocidad de 1 gigabite por segundo.
- **1000Base-SX:** se basa en fibra óptica multimodo y utiliza una longitud de onda corta (la S es por *short*) de 850 nanómetros (770 a 860 nm).

[6] http://html.rincondelvago.com/ethernet_1.html
http://www.mailxmail.com/curso-red-instalacion-fisica/trama-ethernet

La siguiente tabla es un resumen de la tecnología Ethernet.

Tabla 1.1 Estándar Ethernet

Abreviatura	Nombre	Cable	Conector	Velocidad	Puertos
10Base2	Ethernet delgado (Thin Ethernet)	Cable coaxial (50 Ohms) de diámetro delgado	BNC	10 Mb/s	185 m
10Base5	Ethernet grueso (Thick Ethernet)	Cable coaxial de diámetro ancho (10,16 mm)	BNC	10Mb/s	500 m
10Base-T	Ethernet estándar	Par trenzado (categoría 3)	RJ-45	10 Mb/s	100 m
100Base-TX	Ethernet veloz (Fast Ethernet)	Doble par trenzado (categoría 5)	RJ-45	100 Mb/s	100 m
100Base-FX	Ethernet veloz (Fast Ethernet)	Fibra óptica multimodo (tipo 62,5/125)		100 Mb/s	2 km
1000Base-T	Ethernet Gigabit	Doble par trenzado (categoría 5)	RJ-45	1000 Mb/s	100 m
1000Base-LX	Ethernet Giga bit	Fibra óptica mono modo o multimodo		1000 Mb/s	550 m
1000Base-SX	Ethernet Giga bit	Fibra óptica multimodo		1000 Mbit/s	550 m
10GBase-SR	Ethernet de 10 Giga bits	Fibra óptica multimodo		10 Gbit/s	500 m
10GBase-LX4	Ethernet de 10 Giga bits	Fibra óptica multimodo		10 Gbit/s	500 m

1.5.2 TRAMA ETHERNET

El protocolo en el cual está escrito el paquete es el protocolo ETHERNET. En este tipo de paquetes cada trama consta del siguiente formato:

Bytes: 7 1 6 6 2 46-1500 0-46 4

Preámbulo	Inicio del límite De la trama	Dirección del destino	Dirección del origen	Tipo de trama	Datos	Relleno	CRC

Preámbulo: Cada trama empieza por 7 bytes iguales (10101010). Esto permite a los nodos receptores sincronizarse.

- Inicio de trama: Un byte que marca el comienzo de la información propiamente dicho (10101011).
- Dirección del destino: Para saber a quién se le envía el mensaje.
- Dirección del destino: Para saber quién ha enviado el mensaje.
- Tipo de trama: Utilizado para saber el tipo de información que transporta la trama o el protocolo de nivel superior.
- Datos
- Relleno: La norma IEEE 802.3 específica que una trama no puede tener un tamaño inferior a 64 bytes, por tanto, cuando la longitud del campo de datos es muy pequeña se requiere rellenar este campo para completar una trama mínima de al menos 64 bytes. Es un campo que puede, por tanto, tener una longitud comprendida entre 0 y 46 bytes, de modo que la suma total de la trama sea al menos de 64 bytes
- CRC: sirve para hacer detección de errores.

1.5.2 ESTANDAR WIMAX

WiMAX permite la recepción de datos mediante microondas y la retransmisión mediante ondas de radio. Esto facilita el acceso no solo en zonas de población, sino también en zonas aisladas.

También permite llevar las comunicaciones a núcleos de población relativamente pequeños y aislados con costos relativamente económicos, núcleos a los que la telefonía tradicional (por cable) tiene difícil acceso.

Permite además la formación de redes de entorno, pudiendo unir varias redes WiFi, más económicas de implementar, entre sí. Esto, en definitiva, permite la creación de redes de malla, en las que se conectan dos puntos de acceso mediante WiMAX, y a continuación, mediante estos puntos de acceso, dar soporte a una red WiFi (protocolo 802.11).

El estándar utilizado es el 802.16, con sus respectivas variantes. Este estándar está regulado por el WiMAX Forum, asociación sin ánimo de lucro, encargada del desarrollo y control de la compatibilidad e interoperatibilidad de los diferentes elementos que intervienen es esta tecnología (antenas, routers, receptores...).

El estándar IEEE 802.16 hace referencia a un sistema BWA (Broadband Wireless Access) de alta tasa de transmisión de datos y largo alcance (hasta 50-60km), escalable, y que permite trabajar en bandas del espectro tanto "licenciado" como "no licenciado". El servicio, tanto móvil como fijo, se proporciona empleando antenas sectoriales tradicionales o bien antenas adaptativas con modulaciones flexibles que permiten intercambiar ancho de banda por alcance.

Características de wimax:

- Distancias de hasta 80 kilómetros, con antenas muy direccionales y de alta ganancia.
- Velocidades de hasta 75 Mbps, 35+35 Mbps, siempre que el espectro esté completamente limpio.
- Facilidades para añadir más canales, dependiendo de la regulación de cada país.
- Anchos de banda configurables y no cerrados, sujeto a la relación de espectro.

- Permite dividir el canal de comunicación en pequeñas subportadoras (Dos tipos Guardias y Datos).

1.5.3 ESTANDAR WI_FI (WAIFI)

Es un conjunto de redes que no requieren de cables y que funcionan en base a ciertos protocolos previamente establecidos. Si bien fue creado para acceder a redes locales inalámbricas, hoy es muy frecuente que sea utilizado para establecer conexiones a Internet.

Actualmente existen tres tipos de conexiones y hay una cuarta en estudio para ser aprobada que son los siguientes:

- El primero es el estándar IEEE 802.11b que opera en la banda de 2,4 GHz a una velocidad de hasta 11 Mbps.
- El segundo es el IEEE 802.11g que también opera en la banda de 2,4 GHz, pero a una velocidad mayor, alcanzando hasta los 54 Mbps.
- El tercero, que está en uso es el estándar IEEE 802.11 que se le conoce como WiFi 5, ya que opera en la banda de 5 GHz, a una velocidad de 54 Mbps. Una de las principales ventajas de esta conexión es que cuenta con menos interferencias que los que operan en las bandas de 2,4 GHz ya que no comparte la banda de operaciones con otras tecnologías como los Bluetooth.
- El cuarto, y que aún se encuentra en estudio, es el IEEE 802.11n que operaría en la banda de 2,4 GHz a una velocidad de 108 Mbps.

1.6 PROTOCOLOS[7]

Los protocolos son reglas de comunicación que permiten el flujo de información entre equipos que manejan lenguajes distintos, por ejemplo,

[7] http://es.wikipedia.org/wiki/Familia_de_protocolos_de_Internet

dos computadores conectados en la misma red pero con protocolos diferentes no podrían comunicarse jamás, para ello, es necesario que ambas "hablen" el mismo idioma. El protocolo TCP/IP fue creado para las comunicaciones en Internet. Para que cualquier computador se conecte a Internet es necesario que tenga instalado este protocolo de comunicación.

- Estrategias para mejorar la seguridad (autenticación, cifrado).
- Cómo se construye una red física.
- Cómo los computadores se conectan a la red.

En el campo de las redes informáticas, los protocolos se pueden dividir en varias categorías, una de las clasificaciones más estudiadas es la OSI.

Nivel	**Nombre**	**Categoría**
Capa 7	Nivel de aplicación	
Capa 6	Nivel de presentación	Aplicación
Capa 5	Nivel de sesión	
Capa 4	Nivel de transporte	
Capa 3	Nivel de red	
Capa 2	Nivel de enlace de datos	Transporte de datos
Capa 1	Nivel de físico	

Ventajas:

El conjunto TCP/IP está diseñado para enrutar y tiene un grado muy elevado de fiabilidad, es adecuado para redes grandes y medianas, así como en redes empresariales. Se utiliza a nivel mundial para conectarse a Internet y a los servidores web. Es compatible con las herramientas estándar para analizar el funcionamiento de la red.

1.7 ESCANEO

El escáner (del inglés scanner, el que explora o registra) es un aparato o dispositivo utilizado en medicina, electrónica e informática, que explora el

cuerpo humano, un espacio, imágenes o documentos. Su plural es escáneres. Por su ran importancia de algunos dispositivos usados para ciertos trabajos, para este caso se ha escogido una herramienta (Languard Security Scanner) que será de gran ayuda en los laboratorios de redes informáticos en el escaneo de todo una red que se encuentra conectado, esto servirá para detectar y solucionar si algún usuario este con una mala intención o algún puerto o cable se encuentra con problemas, por lo cual se lo podrá solucionar en menor tiempo posible.

CAPITULO 2

EL PROBLEMA

2.1 PLANTEAMIENTO DEL PROBLEMA

Una red de computadoras tiene como objetivo primordial el transmitir y compartir información y recursos a través de la misma, optimizando recursos, tiempo y papeleo a los usuarios que la utilicen, también existen un personal técnico que se encarga de administrar y dar mantenimiento a la red; por lo cual es muy importante tener toda la información de las redes que se gestionan desde el armario principal a todas las redes de distribución y acceso. El laboratorio de Red Informático de las TICs permite la interconexión de todas las áreas, facilitando el uso de las conexiones a cualquier usuario que forme parte de la comunidad Politécnica, brindando servicios de calidad en actividades científicas y de ingeniería.

En los últimos tiempos el hombre ha vivido una impresionante transformación debido al avance de tecnologías de la informática y las telecomunicaciones, es necesaria la documentación administrativa de cada uno de los laboratorios, para lo cual se necesita un diseño estructural que permita tener una visión a futuro del esquema y equipamiento de los laboratorios, dependencias de la comunidad politécnica y su flexibilidad.

Durante el levantamiento de información se pudo observar que los laboratorios de esta institución no cuentan con una documentación de Red, la cual facilitaría la solución de cualquier inconveniente que exista en la misma.

Con la realización de este proyecto, se pretende aportar soluciones a las carencias de monitoreo y escaneo de redes que existe en el Laboratorios

informáticos de Sistemas del bloque Principal de la Escuela Politécnica del Ejército Extensión Latacunga.

2.2 SITUACIÓN ACTUAL

Cada vez la complejidad de los sistemas y nuevas tecnologías implica mayor conocimiento sobre la red, para disminuir fallos en la Red y realizar una tarea completa de diagnostico.

Actualmente los laboratorios Informáticos de Sistemas del bloque Central de la ESPE, cuentan con nueve laboratorios de computación y un departamento administrativo que está ubicado en el último piso de las Aulas. Las mismas que no disponen con la documentación.

2.3 JUSTIFICACION DE LA INVESTIGACION

El Administrador de Red tiene la misión de supervisar y controlar el correcto funcionamiento de la misma tanto administrativa como académica, para lo cual necesita tener a mano toda la información disponible para cuando exista una falla o error en el sistema pueda encontrarlo fácilmente para eso requiere documentar la información de los laboratorios a fin de brindar un mejor control y confiabilidad de la red de datos.

Otra razón que justifica este proyecto que pretendemos llevar a cabo, es que éste representará un aporte al desarrollo de la integración de las redes del núcleo, para lo cual se debe:

- Realizar el plano del laboratorio a efectos de poder esquematizar el cableado.
- Determinar los dispositivos de conexión que serán necesarios para el diseño de la red.
- Ubicar en el edificio el sitio estratégico donde funciona el Cuarto de Comunicaciones y los Cuartos de Equipo instalados.

- Definir el Sistema Operativo de redes que se va a utilizar.

2.4 MÉTODOS DE SUPERVISIÓN DE REDES

2.4.1 Área administrativa

En la parte administrativa debe existir personal capaz de administrar, supervisar y desarrollar las aplicaciones y mantenimiento de la red.

Dentro de los laboratorios informáticos el mantenimiento constara de la verificación del estado del cableado de red así como del buen funcionamiento de las redes o sistemas que hagan uso de la misma, tratando siempre de estar a la vanguardia en cuanto a los sistemas de mejor eficacia y eficiencia en el funcionamiento de la red.

2.4.2 Supervisión de red

Con la utilización del Software (LANguard Network Security Scanner) se realizará un diagnostico de la Red, a fin de que puedan ser examinados para el perfecto funcionamiento de los equipos instalados en cada uno de los laboratorios, a través de este software se puede tener un control permanente de los equipos, evitando así el trafico de Red.

2.4.3 Supervisión del rendimiento

En la ejecución de este software podremos observar en tiempo real diversos sucesos y procesos en la red, con el fin de alcanzar un resultado de datos positivos que ayudan a una buena administración. Para lo cual se establecerá métodos de detección para actividades no autorizadas cuando se produzcan en el futuro.

2.4.4 Visualización de varios equipos

Sí tiene que supervisar varios equipos, ir a cada equipo personalmente puede ser una tarea difícil desde un punto de vista administrativo. La utilidad de (LANguard Network Security Scanner) le permitirá abrir los

registros de datos almacenados y verificar un completo conjunto de características de cada equipo instalado en la red, y el uso de este software proporciona herramientas para ver y administrar varios equipos a la vez.

CAPÍTULO 3

ANÁLISIS Y PROCEDIMIENTOS DE LA INVESTIGACIÓN

3.1 INTRODUCCIÓN

Toda Institución en forma general para su óptimo funcionamiento requiere de un sistema de cableado. El cable se instala normalmente en edificios por intermedio de canaletas o tubos subterráneos, los cables metálicos y coaxiales utilizan el cobre como principal material de transmisión para las redes, los cables metálicos están formados por hilos de par trenzado. El cable de fibra óptica se encuentra disponible con filamentos sencillos o múltiples, de plástico o de fibra de cristal.

Aunque el cableado parezca el componente más simple de una red puede ser el más costoso, comprometiendo hasta un 50% del presupuesto total de la implementación. El cableado también puede ser la mayor fuente de problemas que se presentan en la red, tanto en su instalación como en su mantenimiento, por lo tanto al hacer la instalación el cableado debe ser tomado muy en serio, ya que la mala elección o la mala instalación puede ocasionar pérdidas en un futuro cercano o probablemente no se tenga la oportunidad de volver hacer esta inversión nuevamente.

El cableado seleccionado para la red debe ser capaz de transmitir cantidades masivas a grandes velocidades y a través de grandes distancias. Esta capacidad es llamada "Ancho de Banda", que es importante para la transmisión de multimedia a través de la red.

3.2 ANÁLISIS DE REQUERIMIENTOS DE USUARIOS

Tabla 3.2. Requerimientos del sistema Internetworking

REQUERIMIENTOS DEL USUARIO	**DESCRIPCIÓN**
Localización (es) y número (s) de usuarios	ESPE-LATACUNGA - 2 Administrativos - 750 Usuarios (semanales)
Crecimiento esperado en el número de usuarios	
Después de un año	1 % de usuarios
Después de dos años	5 % de usuarios
Expectativas del usuario	
Interactividad	Los usuarios esperan un comportamiento de la red excelente que les permita tener disponibilidad de los servicios de forma rápida e ininterrumpida.
Calidad	La red deberá tener alta calidad en la transmisión de datos, dando prioridad a las aplicaciones de voz y video
Flexibilidad	La red deberá adaptarse fácilmente a los cambios de ubicación de usuarios de los mismos.
Seguridad	La red deberá contar con un alto grado de seguridad, para evitar congestiones en la red

3.3 ANÁLISIS Y DIAGNÓSTICO DE LA INFRAESTRUCTURA DE INTERCONEXIÓN

La red de cableado estructurado existente en el Laboratorio de Sistemas del Bloque Central 4 piso de la ESPE-L tiene 4 salidas de datos conectados a cuatro distribuidores de red por medio de cable de fibra óptica y cable UTP de cobre.

3.3.1 DESCRIPCIÓN

El backbone de la Red de Laboratorio de Sistemas del bloque Central 4 piso de la ESPE-L, se enlaza a 3 subredes LAN, con tecnología

Fastethernet. La distribución principal esta implementada en el CENTRO DE DATOS 1 La salida a la Red WAN se realiza mediante enlace dedicado, que permite conectar a la ESPE Matriz en Sangolquí, con todas las Extensiones. Esto se realiza a través de un Firewall empleando también un Router. En base a coordinaciones realizadas con el personal de redes de la Unidad TIC´s de la ESPE Matriz. (Ver Figura 3.1)

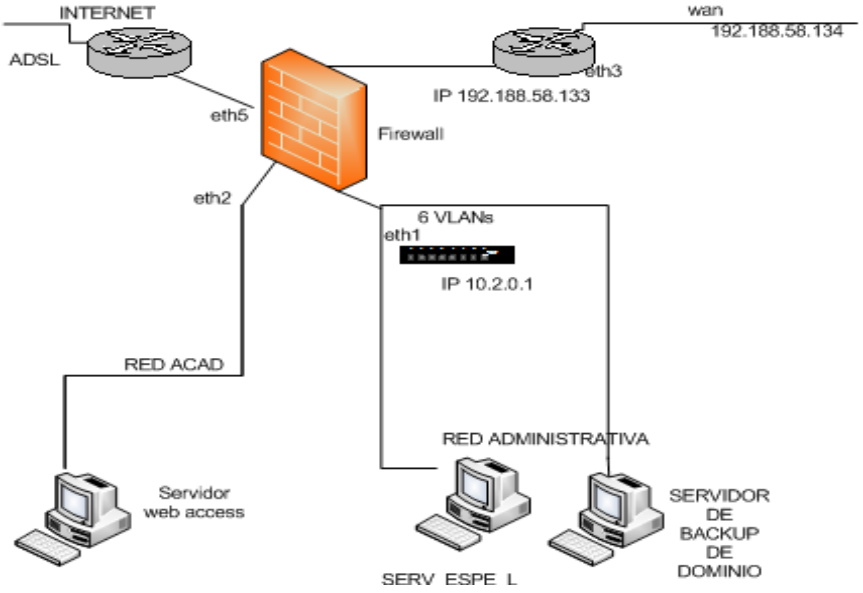


Figura 3.1. Topología Física de la red de datos de la ESPEL

La integración de los Switchs de interconexión se realiza a través de un Firewall que dispone de 6 tarjetas de red Fastethernet 10/100 MHz.

EL switch que realiza las veces de CORE es un SWITCH CISCO catalyst 2950, mismo que tiene configurad 1 VLANS (Red Académica), que distribuye a cada uno de los laboratorios. El Switch de CORE tiene una conexiones de fibra que conecta al centros de dato TICs.

El Laboratorio de Sistemas dispone de un Firewall bastante robusto que trabaja a nivel de la capa de aplicación denominado CHECK POINT.

3.3.2 AREA DE DISTRIBUIDORES

3.3.2.1 DISTRIBUIDOR PRINCIPAL

Existe un distribuidor principal ubicado en el bloque Central en la planta baja del edificio antiguo (código EA-BB-23-PB)[8]. Este distribuidor está compuesto por un rack de 42U[9] tipo abierto en el que se encuentran paneles de conexión (patch panels) de 16, 24 y 48 puertos RJ45 Categoría 5e, un panel de fibra óptica de 24 puertos, organizadores horizontales y verticales para la administración de los cables de red horizontal y de interconexión, equipos activos de red y multitomas eléctricas, conforme se indica en el diagrama de rack figura 3.2. Estos componentes son de varias marcas.

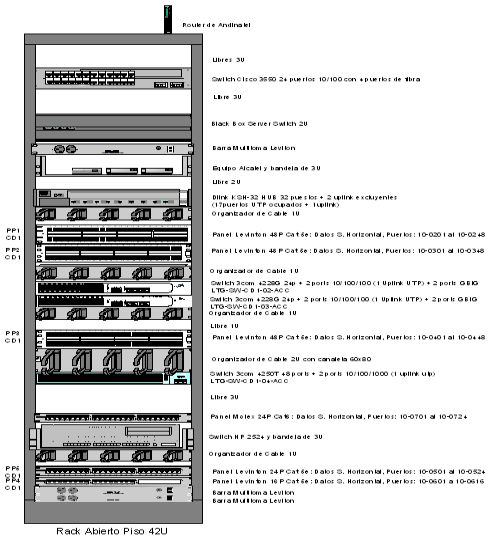


Figura 3.2. Esquema distribuidor MDF[10] – 10 – Centro de Datos.

Existe una rotulación de los cables UTP que permite su identificación. La codificación de esta rotulación está relacionada con la función del área a la

[8] código dado por el departamento de construcciones
[9] 42 unidades
[10] Distribuidor Principal

que conecta el cable. A continuación observamos la red del cableado del laboratorio de sistemas en la figura 3.3

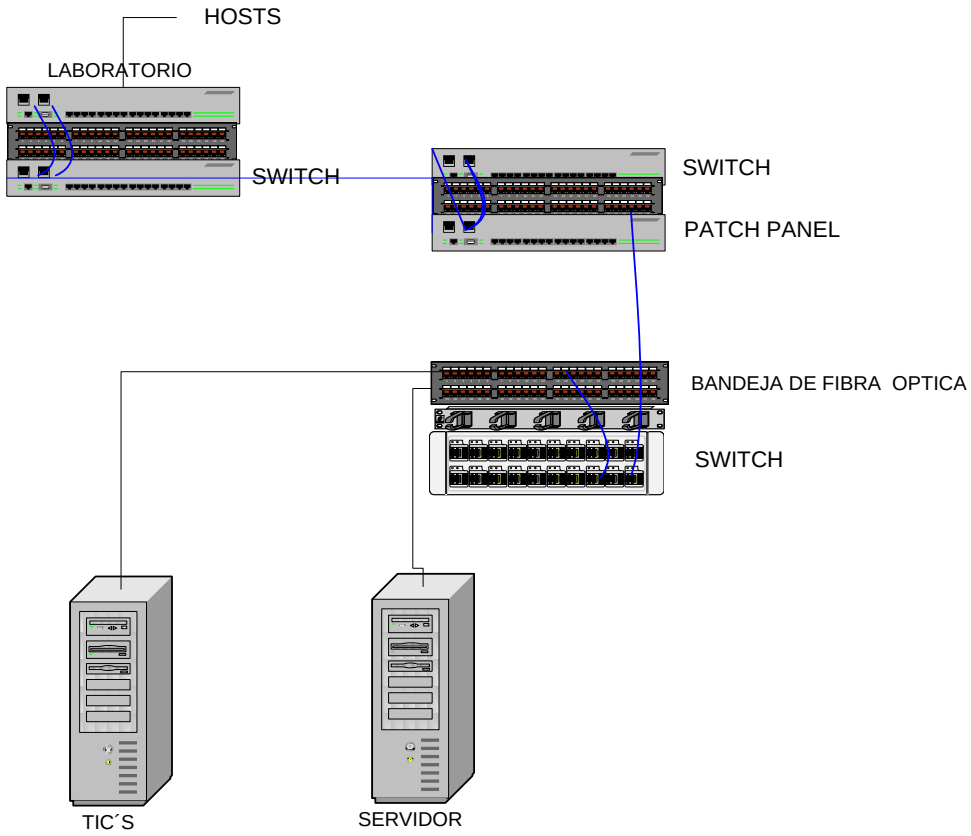


Figura 3.3. Esquema distribuidor con el Laboratorio de Sistemas.

3.3.2.2 DISTRIBUIDORES SECUNDARIOS

Un distribuidor ubicado en el Piso 3 (cuarta planta) del Edificio de Aulas y Laboratorios (bloque de gradas, código BG-BB-1-P4), en la Oficina de Laboratorios. Desde el distribuidor principal llega un cable de fibra óptica de 4 fibras MM que se conecta al trancybers[11], está a su vez se conecta directamente al equipo Switch atreves del cable UTP de 4 pares Cat. 5e. Donde se encuentran conectados los 9 laboratorios, ubicándose 5 laboratorios en el edificio del bloque A “SOLDADO MOLINA NESTOR”

[11] Trasforma de fibra óptica a Utp

y 4 laboratorios en el bloque B “LA NUEVA PATRIA” para ser controlado por un servidor, y un cable UTP que conecta con el distribuidor ubicado en el bloque de graderíos. A continuación en las tablas 3.2 y 3.3 vemos en detalle los puertos del MDF – 40 y del Switch Catalyst 2950 respectivamente.

Tabla 3.2. Detalle de puertos del Patch Panel MDF – 40

PATCH PANEL MDF - 40 DISTRIBUIDOR PRINCIPAL	
LABORATORIOS	**PUERTOS**
INGENIERIA DE SOFTWARE	01
COMPUTACION II	02
COMPUTACION I	03
REDES DE DATOS I	04
LENGUAJE DE PROGRAMACION	05
CIENCIAS ADMINISTRATIVAS	06
CIANCIAS ADMINISTRATIVAS	07
OFICINAS	08
REDES DE DATOS II	09

Tabla 3.3. Detalle de puertos del Switch Catalyst 2950

SWITCH SYSTEM-CATALYS 2950		
LABORATORIOS	**PUERTO**	**COLOR**
SWITCH PROGRAMABLE	01	PLOMO
REDES DE DATOS I	05	ROJO
REDES DE DATOS II	06	ROJO
INGENIERIA DE SOFTWARE	07	ROJO
COMPUTACION III	09	ROJO
OFICINAS	10	ROJO
LENGUAJE DE PROGRAMACION	11	ROJO
CIENCIAS ADMINISTRATIVAS	12	ROJO
SERVIDOR DE ARCHIVOS	14	AZUL
CONTROLADOR DE DOMINIO	15	AZUL
ANTIVIRUS	16	AZUL
FIREWALL	17	AZUL
TRANCYBERS	23	ROJO

Este distribuidor está formado por un rack abierto de 6U, de montaje en pared, un panel de conexión de 16 y otro de 24 puertos RJ45 C5e y equipos como se indica en la figura 3.4.

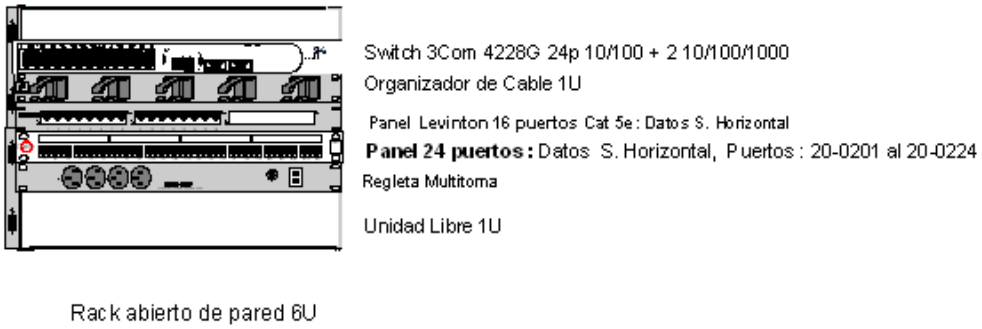


Figura 3.4. Esquema Distribuidor MDF

Al equipo Switch se conecta directamente el cable de backbone de fibra óptica que llega desde el distribuidor principal. Y de los paneles de conexión se conectan cables UTP a las áreas de trabajo del edificio.

Los cordones de conexión (patch cords) utilizados para la interconexión de los paneles de conexión con los equipos Switch son en su mayoría hechos en fábrica (como indica las normas), de cable UTP 4 pares multifilar, con plugs RJ45 en sus extremos, de Categoría 5e.

3.3.2.3 CABLEADO DE BACKBONE

El backbone existente está formado por dos cables de fibra óptica multimodo de 4 fibras cada uno, tipo Armored, que conecta al distribuidor principal con el distribuidor (Switch) del edificio de Aulas y Laboratorios.

Los cables de backbone se encuentran instalados por medio de tuberías enterradas (canalizaciones) que conectan los edificios en cuestión. Existen posos y cajas de revisión a lo largo del recorrido de la canalización que facilita el movimiento de cables en nuevas instalaciones. (Ver Figura 3.5)

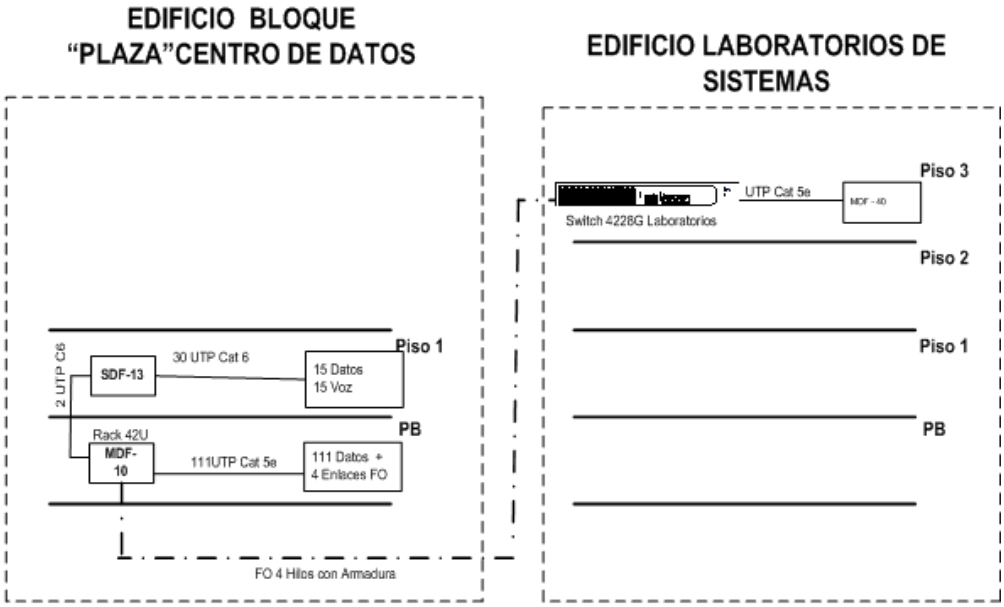


Figura 3.5. Esquema del Cableado Horizontal y Backbone de la Red

3.3.2.4 CABLEADO HORIZONTAL Y AREA DE TRABAJO

La red de cableado entre los distribuidores y las áreas de trabajo en los Laboratorios de sistemas del bloque Central de la ESPEL, está realizado con cables UTP de 4 pares Categoría 5 y 5e de chaqueta PVC, en su mayoría conectados a paneles de conexión en el extremo del distribuidor y a placas de puertos RJ45 C5e en el extremo del área de trabajo. Ambos extremos del cable UTP se encuentran rotulados en su mayor parte. Los cables son llevados en su mayor parte por medio de tuberías empotradas en pisos o paredes. Los recorridos troncales se los hace por tuberías PVC de 1" a 4" y terminar con tuberías o mangueras de menor calibre desde las cajas de paso ubicadas en posiciones convenientes. Cuando no es posible el uso de tuberías se tienen instaladas canaletas decorativas de varios calibres para la conducción de cables hasta llegar a placas sobrepuestas en las estaciones de trabajo. Las placas con puertos RJ45 C5e utilizadas son de varias marcas y tienen en su mayor parte rotulaciones para su identificación.

También existen cables UTP conectados directamente a plugs RJ45 en su extremo (no cumple las normas de instalación) y que se conectan directamente a equipos activos (Switch o Hubs) en la oficina de Laboratorios (edificio Aulas y Laboratorios).

Los cordones de conexión (patch cords) utilizados para la interconexión entre las salidas (placas de puertos RJ45) con los computadores son en su mayoría hechos en fábrica (como indica las normas), de cable UTP 4 pares multifilar, con plugs RJ45 en sus extremos, de Categoría 5e.

A continuación en la figura 3.6., indicaremos el Área de trabajo de nuestro estudio:

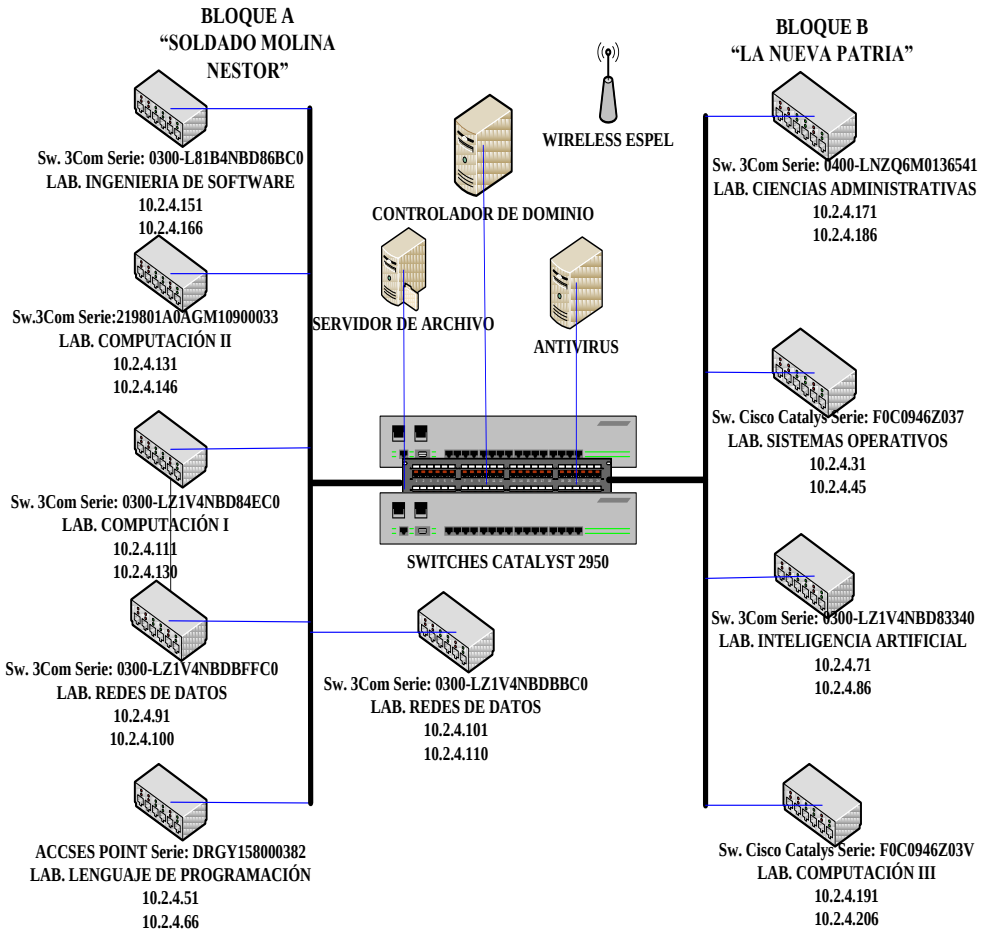


Figura 3.6. Red Física de la Red de datos (Laboratorios Informáticos)

3.3.2.5 TECNOLOGÍAS

La tecnología actual disponible en la red LAN es Fast Ethernet para poder reutilizar la mayor cantidad de elementos activos y en función de la tecnología actual de mercado, se dispone de tecnología G*igabit Ethernet* para el backbone (core) que permite satisfacer los requerimientos del Internetworking de la red. Gigabit Ethernet todavía conserva el formato de tramas y tamaños de la trama y utiliza CSMA/CD[12]. Al igual que las tecnologías anteriores, es posible el funcionamiento full dúplex. La tabla 3.4 indica las características más importantes que permiten seleccionar la interface física (GBIC) de conexión más adecuada para cada nodo de la red.

Tabla 3.4: Características de Escalabilidad en Giga bit Ethernet

TIPO	**VELOCIDAD**	**MÁXIMA LONGITUD DE SEGMENTO**	**CODIFICACION**	**MEDIO FISICO**
1000Base T	1000 Mbps	100 m	Nivel-5	UTP Cat. 5
1000BaseLX (onda larga)	1000 Mbps	550 m	8B/10B	Fibra multi/mono modo
1000BaseSX (onda corta)	1000 Mbps	62.5 μm, 220 m50 μm, 500 m	8B/10B	Fibra multimodo
1000BaseCX	1000 Mbps	25 m	8B/10B	Cobre blindado

[12] Acceso múltiple con detección de portadora y detección de colisiones. Que tiene la capacidad de detectar los errores que resulten al trasmitir simultáneamente varias estaciones.

3.3.2.6 DIRECCIONAMIENTO IP DE LA RED DE DATOS DE LOS LABORATORIOS DE SISTEMAS

A continuación se detalla la información obtenida durante la recopilación de datos de cada uno de los laboratorios, que fue posible gracias a la colaboración del personal técnico y administrativo de la RED LAN.

DETALLE GENERAL DE LOS LABORATORIOS DE REDES INFORMATICO

Todos los laboratorios de redes informático se encuentran con una interface de Dominio (LABINF), DNS (10.2.4.7), y Gateway (10.2.4.8). Los mimos que tienen su horario de funcionamiento ininterrumpido de lunes a viernes de 07:00 am a 21:30 pm.

DETALLE POR LABORATORIOS

LABORATORIO 01 "INGENIERIA DE SOFTWARE"

Este laboratorio consta de 01Patch Panel, 01 Switch (3Com Serie: 0300-L81B4NBD86BC0), y 16 Host. La interface al distribuidor principal es el puerto 01.

SOFTWARE INSTALADOS

Win Xp Sp3, Office 2007, Visual Basic 6.0, Winzip, Acrobat Reader 5.0

Tabla 3.5: Detalles de los Equipos del Laboratorio N'01

DETALLE DE LOS EQUIPOS			
NOMBRE DEL EQUIPO	**DIRECCION IP**	**DIRECCION MAC**	**NOMINATIVO**
LTG-LAB-ISO1	10.2.4.151	00-1C-C0-DE-08-58	LIS-001
LTG-LAB-ISO2	10.2.4.152	00-1C-C0-E0-2A-D9	LIS-002
LTG-LAB-ISO3	10.2.4.153	00-1C-C0-E0-2A-E5	LIS-003
LTG-LAB-ISO4	10.2.4.154	00-21-91-53-15-C6	LIS-004
LTG-LAB-ISO5	10.2.4.155	00-1C-C0-E0-2A-65	LIS-005
LTG-LAB-ISO6	10.2.4.156	00-1C-CO-E0-2A-C7	LIS-006
LTG-LAB-ISO7	10.2.4.157	00-1C-C0-E0-2A-AD	LIS-007

LTG-LAB-ISO8	10.2.4.158	00-1C-C0-E0-2A-C3	LIS-008
LTG-LAB-ISO9	10.2.4.159	00-1C-C0-E0-24-2F	LIS-009
LTG-LAB-ISO10	10.2.4.160	00-1C-C0-DE-09-7F	LIS-010
LTG-LAB-ISO11	10.2.4.161	00-1C-CO-E0-2A-14	LIS-011
LTG-LAB-ISO12	10.2.4.162	00-1C-C0-E0-2A-1A	LIS-012
LTG-LAB-ISO13	10.2.4.163	00-1C-C0-E0-2A-5A	LIS-013
LTG-LAB-ISO14	10.2.4.164	00-1C-C0-E0-2A-70	LIS-014
LTG-LAB-ISO15	10.2.4.165	00-27-0E-0F-74-6D	LIS-015
LTG-LAB-ISO16	10.2.4.166	00-27-0E-0F-74-5A	LIS-016

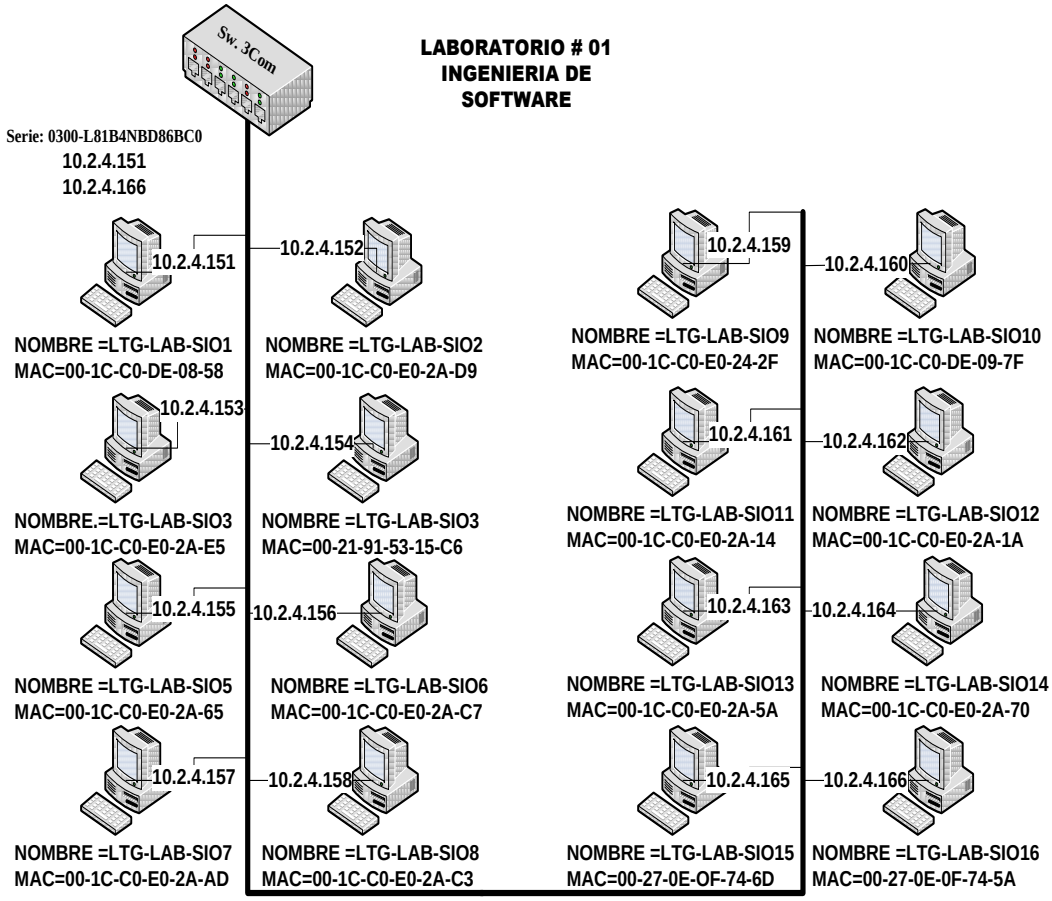


Figura 3.7. Red Física del Laboratorio N'01

LABORATORIO No 02 "COMPUTACIÓN II"

Este laboratorio consta de 01Patch Panel, 01 Switch (Sw.3Com Serie: 219801A0AGM10900033), y 16 Host. La interface al distribuidor principal es el puerto 02.

SOFTWARE INSTALADOS

Win Xp Sp3, Office 2007, Visual Basic 6.0, Winzip, Acrobat Reader 5.0

Tabla 3.6: Detalles de los Equipos del Laboratorio N'02.

DETALLE DE LOS EQUIPOS			
NOMBRE DEL EQUIPO	**DIRECCION IP**	**DIRECCION MAC**	**NOMINATIVO**
LTG-LAB-MII1	10.2.4.131	00-21-5A-E7-90-98	LC2-001
LTG-LAB-MII2	10.2.4.132	00-21-5A-E7-90-A8	LC2-002
LTG-LAB-MII3	10.2.4.133	00-21-5A-E7-90-A1	LC2-003
LTG-LAB-MII4	10.2.4.134	00-21-5A-E7-97-BE	LC2-004
LTG-LAB-MII5	10.2.4.135	00-21-5A-E7-97-75	LC2-005
LTG-LAB-MII6	10.2.4.136	00-21-5A-E7-97-A3	LC2-006
LTG-LAB-MII7	10.2.4.137	00-21-5A-E7-90-A2	LC2-007
LTG-LAB-MII8	10.2.4.138	00-21-5A-E7-97-8F	LC2-008
LTG-LAB-MII9	10.2.4.139	00-21-5A-E7-13-EE	LC2-009
LTG-LAB-MII10	10.2.4.140	00-21-5A-E7-97-79	LC2-010
LTG-LAB-MII11	10.2.4.141	00-21-5A-E7-90-27	LC2-011
LTG-LAB-MII12	10.2.4.142	00-21-5A-E7-90-21	LC2-012
LTG-LAB-MII13	10.2.4.143	00-21-5A-E7-90-43	LC2-013
LTG-LAB-MII14	10.2.4.144	00-21-5A-E7-90-9E	LC2-014
LTG-LAB-MII15	10.2.4.145	00-27-0E-0F-74-52	LC2-015
LTG-LAB-MII16	10.2.4.146	00-27-0E-0F-86-1F	LC2-016

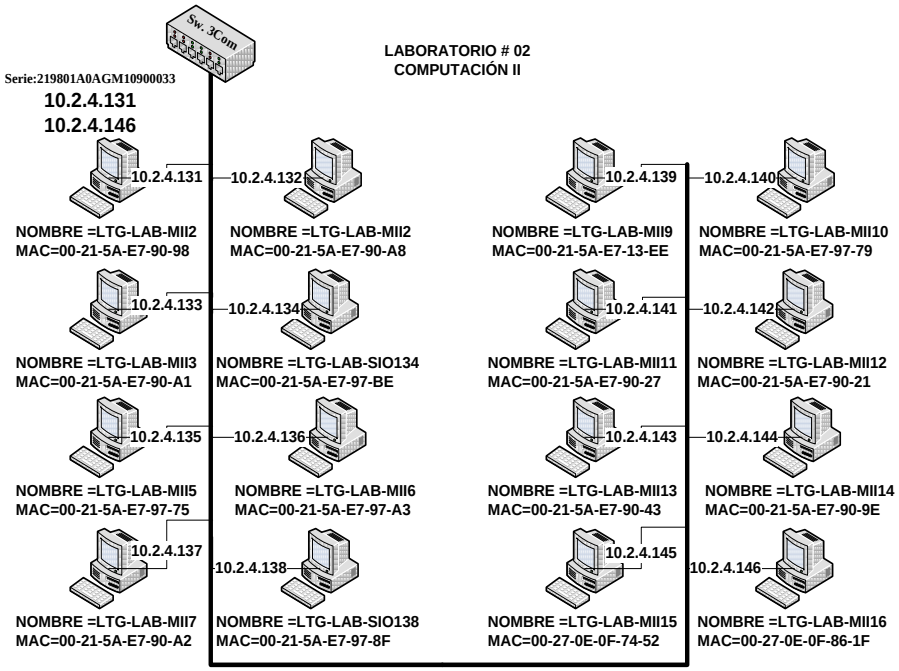


Figura 3.8. Red Física del Laboratorio N'02.

LABORATORIO No 03 "COMPUTACIÓN I"

Este laboratorio consta de 01Patch Panel, 01 Switch (Sw. 3Com Serie: 0300-LZ1V4NBD84EC0), y 16 Host. La interface al distribuidor principal es el puerto 03.

SOFTWARE INSTALADOS

Win Xp Sp3, Office 2007, Visual Basic 6.0, Winzip, Acrobat Reader 5.0

Tabla 3.7: Detalles de los Equipos del Laboratorio N'03

DETALLE DE LOS EQUIPOS			
NOMBRE DEL EQUIPO	**DIRECCION IP**	**DIRECCION MAC**	**NOMINATIVO**
LTG-LAB-MI1	10.2.4.111	00-1C-C0-16-D7-16	LC1-001
LTG-LAB-MI2	10.2.4.112	00-1C-CO-16-D7-3A	LC1-002
LTG-LAB-MI3	10.2.4.113	00-1C-CO-17-DE-3E	LC1-003
LTG-LAB-MI4	10.2.4.114	00-1C-CO-16-D7-4C	LC1-004
LTG-LAB-MI5	10.2.4.115	00-1C-CO-16-F0-DA	LC1-005
LTG-LAB-MI6	10.2.4.116	00-1C-C0-17-E0-83	LC1-006

LTG-LAB-MI7	10.2.4.117	00-1C-C0-16-F0-D7	LC1-007
LTG-LAB-MI8	10.2.4.118	00-1C-C0-17-E0-B4	LC1-008
LTG-LAB-MI9	10.2.4.119	00-1C-C0-17-DD-57	LC1-009
LTG-LAB-MI10	10.2.4.120	00-1C-C0-17-DB-4C	LC1-010
LTG-LAB-MI11	10.2.4.121	00-1C-C0-17-DD-C6	LC1-011
LTG-LAB-MI12	10.2.4.122	NO INICIA EL CPU	LC1-012
LTG-LAB-MI13	10.2.4.123	00-1C-CO-17-DE-71	LC1-013
LTG-LAB-MI14	10.2.4.124	00-1C-CO-17-DC-AD	LC1-014
LTG-LAB-MI15	10.2.4.125	00-EO-4D-58-83-91	LC1-015
LTG-LAB-MI16	10.2.4.126	00-OC-76-5C-63-18	LC1-016
LTG-LAB-MI17	10.2.4.127	00-1C-CO-16-FO-DO	LC1-017
LTG-LAB-MI18	10.2.4.128	00-19-21-56-AE-78	LC1-018
LTG-LAB-MI19	10.2.4.129	00-1C-CO-17-DE-9B	LC1-019
LTG-LAB-MI20	10.2.4.130	NO TIENE CPU	LC-020

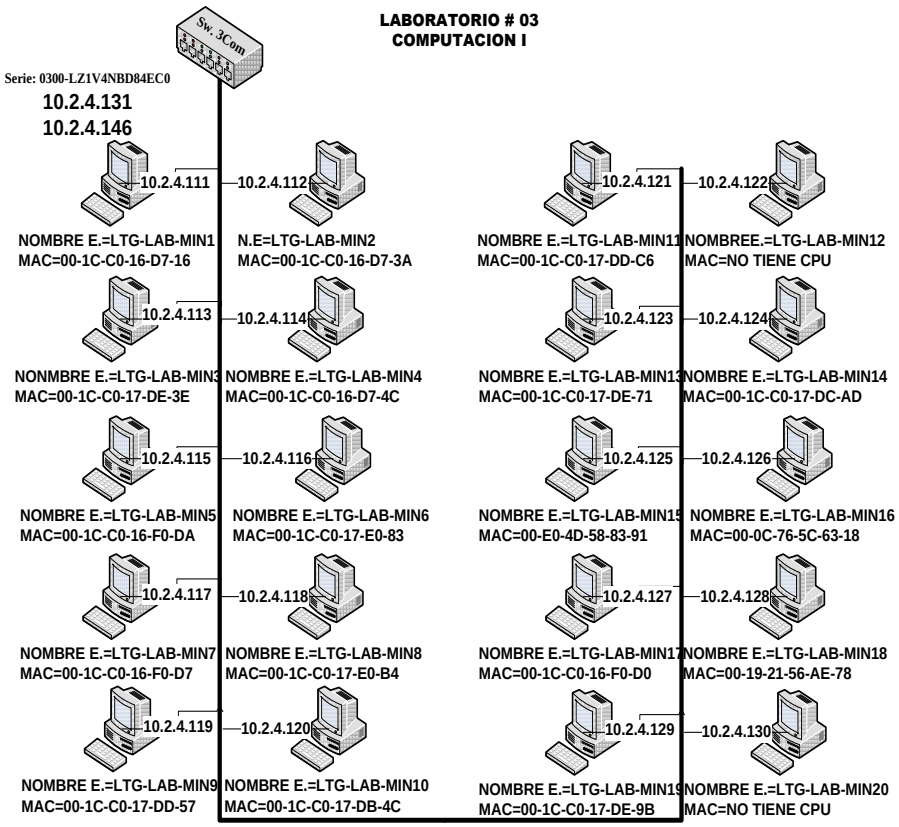


Figura 3.9. Red Física del Laboratorio N'03.

LABORATORIO No 04 "REDES DE DATOS"

Este laboratorio consta de 01Patch Panel, 02 Switch (Sw.3Com Serie: 219801A0AGM10900033 Y Sw. Serie: 0300-LZ1V4NBDBBC0), y 16 Host. La interface al distribuidor principal es el puerto 04.

SOFTWARE INSTALADOS

Win Xp Sp3, Office 2007, Visual Basic 6.0, Winzip, Acrobat Reader 5.0

Tabla 3.8: Detalles de los Equipos del Laboratorio N'04

DETALLE DE LOS EQUIPOS			
NOMBRE DEL EQUIPO	**DIRECCION IP**	**DIRECCION MAC**	**NOMINATIVO**
LTG-LAB-RED1	10.2.4.91	00-16-76-00-7B-F4	LRD-001
LTG-LAB-RED2	10.2.4.92	00-16-76-00-54-C0	LRD-002
LTG-LAB-RED3	10.2.4.93	00-19-D1-81-8B-EE	LRD-003
LTG-LAB-RED4	10.2.4.94	00-16-76-00-54-4E	LRD-004
LTG-LAB-RED5	10.2.4.95	00-16-76-00-7A-1F	LRD-005
LTG-LAB-RED6	10.2.4.96	00-16-76-00-79-A7	LRD-006
LTG-LAB-RED7	10.2.4.97	00-16-76-00-53-36	LRD-007
LTG-LAB-RED8	10.2.4.98	00-16-76-00-57-CC	LRD-008
LTG-LAB-RED9	10.2.4.99	00-16-76-00-5E-0F	LRD-009
LTG-LAB-RED10	10.2.4.100	00-16-76-00-56-74	LRD-010
LTG-LAB-RED11	10.2.4.101	NO TIENE CPU	LRD-011
LTG-LAB-RED12	10.2.4.102	00-16-76-00-57-56	LRD-012
LTG-LAB-RED13	10.2.4.103	00-16-76-00-54-98	LRD-013
LTG-LAB-RED14	10.2.4.104	00-16-76-00-54-CB	LRD-014
LTG-LAB-RED15	10.2.4.105	00-16-76-00-56-D0	LRD-015
LTG-LAB-RED16	10.2.4.106	00-16-76-00-55-9C	LRD-016
LTG-LAB-RED17	10.2.4.107	00-16-76-00-7B-94	LRD-017
LTG-LAB-RED18	10.2.4.108	00-16-76-00-55-57	LRD-018
LTG-LAB-RED19	10.2.4.109	00-16-76-00-57-9F	LRD-019
LTG-LAB-RED20	10.2.4.110	00-27-0E-0F-8A-8F	LRD-020

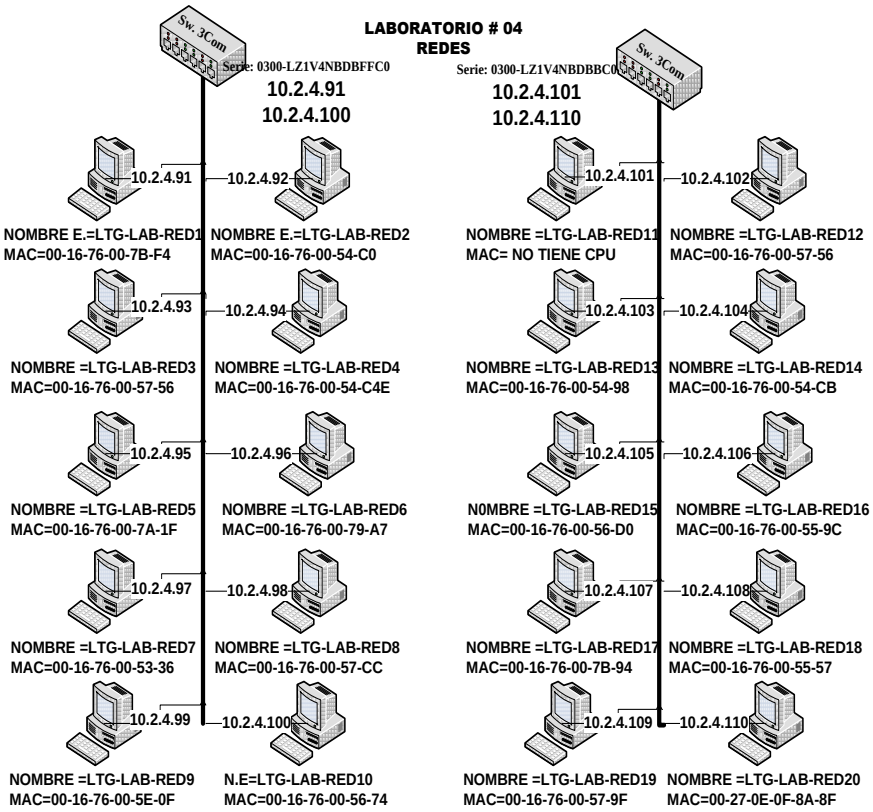


Figura 3.10. Red Física del Laboratorio N'04

LABORATORIO No 05 "LENGUAJE DE PROGRAMACIÓN"

Este laboratorio consta de 01Patch Panel, 01Accses Point (Serie: DRGY158000382), y 16 Host. La interface al distribuidor principal es el puerto 05.

SOFTWARE INSTALADOS

Win Xp Sp3, Office 2007, Visual Basic 6.0, Winzip, Acrobat Reader 5.0

Tabla 3.9: Detalles de los Equipos del Laboratorio N'05

DETALLE DE LOS EQUIPOS			
NOMBRE DEL EQUIPO	**DIRECCION IP**	**DIRECCION MAC**	**NOMINATIVO**
LTG-LAB-LGP1	10.2.4.51	00-0D-88-A8-3B-D1	LLP-001
LTG-LAB-LGP2	10.2.4.52	00-0D-88-A6-67-1D	LLP-002
LTG-LAB-LGP3	10.2.4.53	00-13-46-70-08-4E	LLP-003

LTG-LAB-LGP4	10.2.4.54	00-13-46-70-07-E1	LLP-004
LTG-LAB-LGP5	10.2.4.55	00-1B-11-1C-9D-14	LLP-005
LTG-LAB-LGP6	10.2.4.56	00-1B-11-1C-9D-1B	LLP-006
LTG-LAB-LGP7	10.2.4.57	00-1B-11-18-F0-6B	LLP-007
LTG-LAB-LGP8	10.2.4.58	00-1B-11-1A-C3-79	LLP-008
LTG-LAB-LGP9	10.2.4.59	00-0D-88-A6-67-02	LLP-009
LTG-LAB-LGP10	10.2.4.60	00-0D-88-9D-38-E1	LLP-010
LTG-LAB-LGP11	10.2.4.61	00-13-46-70-07-97	LLP-011
LTG-LAB-LGP12	10.2.4.62	00-13-46-70-04-EC	LLP-012
LTG-LAB-LGP13	10.2.4.63	00-1B-11-18-F0-6C	LLP-013
LTG-LAB-LGP14	10.2.4.64	00-17-9A-0A-95-5E	LLP-014
LTG-LAB-LGP15	10.2.4.65	00-1B-11-1C-9D-16	LLP-015
LTG-LAB-LGP16	10.2.4.66	00-1B-11-1A-BD-1F	LLP-016

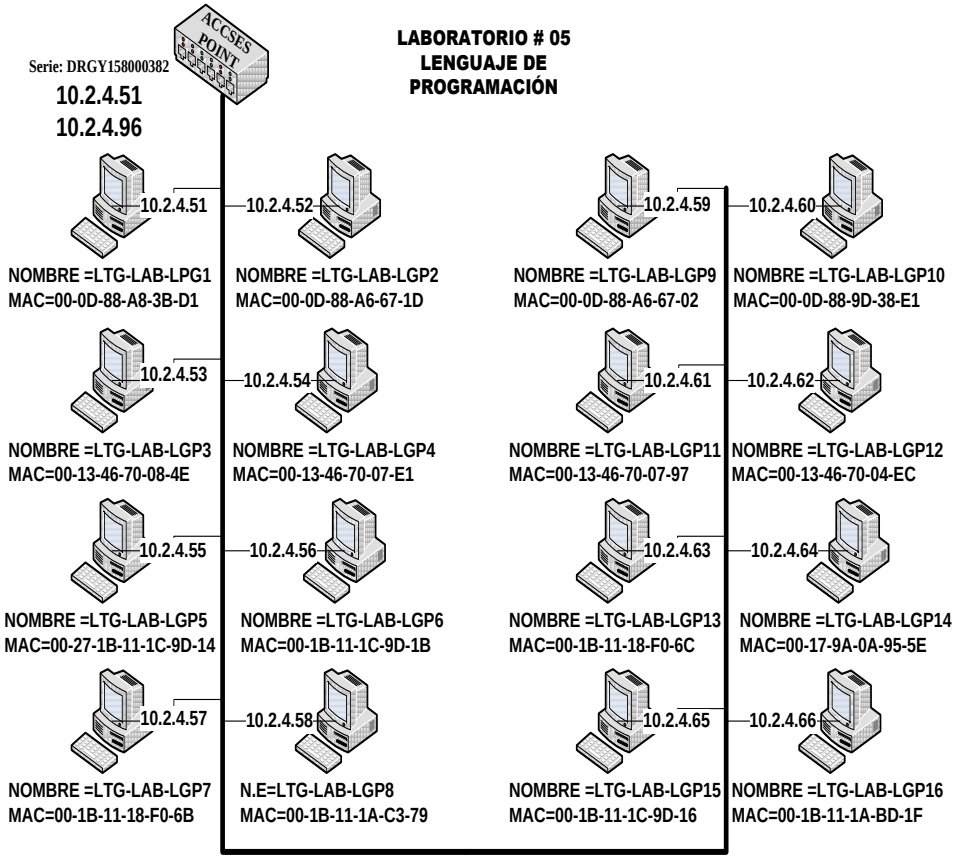


Figura 3.11. Red Física del Laboratorio N’05

LABORATORIO No 06 "CIENCIAS ADMINISTRATIVAS"

Este laboratorio consta de 01Patch Panel, 01 Switch (Sw. 3Com Serie: 0400-LNZQ6M0136541), y 16 Host. La interface al distribuidor principal es el puerto 06.

SOFTWARE INSTALADOS

Win Xp Sp3, Office 2007, Visual Basic 6.0, Winzip, Acrobat Reader 5.0

Tabla 3.10: Detalles de los Equipos del Laboratorio N'06

DETALLE DE LOS EQUIPOS			
NOMBRE DEL EQUIPO	**DIRECCION IP**	**DIRECCION MAC**	**NOMINATIVO**
LTG-LAB-CIA1	10.2.4.171	00-04-75-C1-41-7C	LCA-001
LTG-LAB-CIA2	10.2.4.172	00-1C-C0-17-BF-EF	LCA-002
LTG-LAB-CIA3	10.2.4.173	00-16-76-BB-5F-2F	LCA-003
LTG-LAB-CIA4	10.2.4.174	00-04-75-C1-41-59	LCA-004
LTG-LAB-CIA5	10.2.4.175	00-16-76-BB-5B-2C	LCA-005
LTG-LAB-CIA6	10.2.4.176	00-16-76-BB-5B-55	LCA-006
LTG-LAB-CIA7	10.2.4.177	00-1C-C0-17-E0-5A	LCA-007
LTG-LAB-CIA8	10.2.4.178	00-1C-C0-16-CE-CB	LCA-008
LTG-LAB-CIA9	10.2.4.179	00-04-75-C1-40-D0	LCA-009
LTG-LAB-CIA10	10.2.4.180	00-16-76-BB-5D-DD	LCA-010
LTG-LAB-CIA11	10.2.4.181	00-16-76-BB-5C-78	LCA-011
LTG-LAB-CIA12	10.2.4.182	00-04-75-C1-3F-8E	LCA-012
LTG-LAB-CIA13	10.2.4.183	00-04-75-C1-41-53	LCA-013
LTG-LAB-CIA14	10.2.4.184	00-04-75-C1-40-CD	LCA-014
LTG-LAB-CIA15	10.2.4.185	00-04-75-C1-3F-91	LCA-015
LTG-LAB-CIA16	10.2.4.186	00-04-75-C1-40-5B	LCA-016

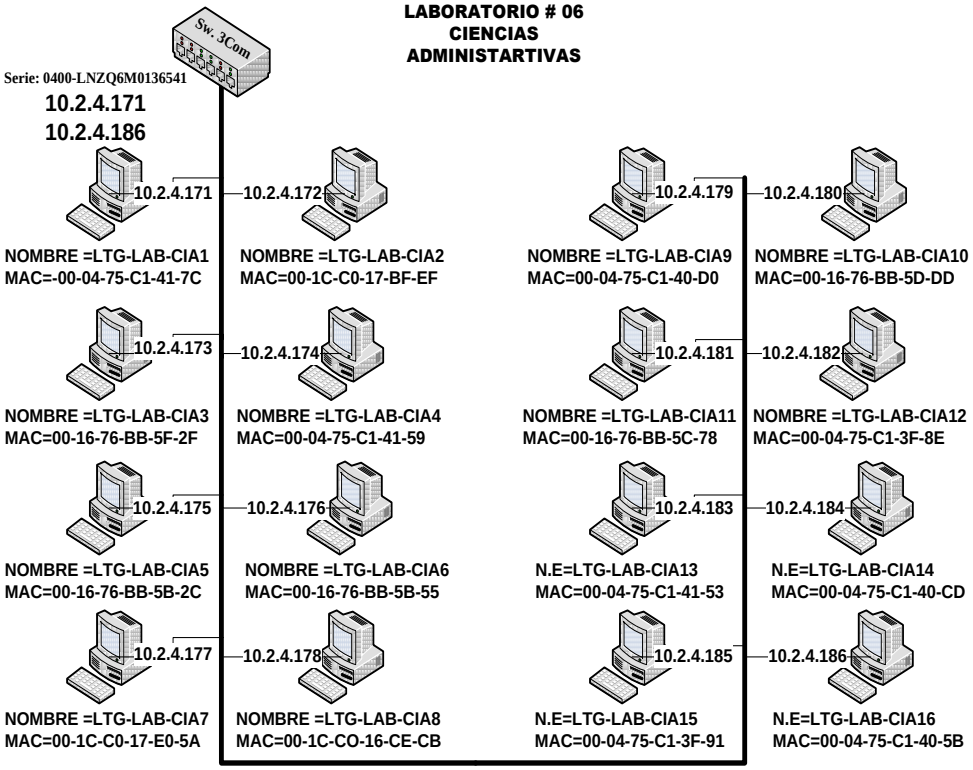


Figura 3.12. Red Física del Laboratorio N'06

LABORATORIO No 07 "SISTEMAS OPERATIVOS"

Este laboratorio consta de 01Patch Panel, 01 Switch (Sw. Cisco Catalys Serie: F0C0946Z037), y 16 Host. La interface al distribuidor principal es el puerto 07.

SOFTWARE INSTALADOS

Win Xp Sp3, Linux, Office 2007, Visual Basic 6.0, Winzip, Acrobat Reader 5.0

Tabla 3.11: Detalles de los Equipos del Laboratorio N'07

DETALLE DE LOS EQUIPOS			
NOMBRE DEL EQUIPO	**DIRECCION IP**	**DIRECCION MAC**	**NOMINATIVO**
LTG-LAB-SIO1	10.2.4.31	00-1C-C0-F1-01-7D	LSO-001
LTG-LAB-SIO2	10.2.4.32	00-27-0E-0F-86-6A	LSO-002

LTG-LAB-SIO3	10.2.4.33	00-1C-C0-F1-4C-5B	LSO-003
LTG-LAB-SIO4	10.2.4.34	00-27-0E-0F-86-45	LSO-004
LTG-LAB-SIO5	10.2.4.35	00-1C-C0-F1-4A-15	LSO-005
LTG-LAB-SIO6	10.2.4.36	00-1C-C0-F1-01-4C	LSO-006
LTG-LAB-SIO7	10.2.4.37	00-27-0E-0F-86-6D	LSO-007
LTG-LAB-SIO8	10.2.4.38	00-1C-C0-F1-01-98	LSO-008
LTG-LAB-SIO9	10.2.4.39	00-27-0E-0F-86-44	LSO-009
LTG-LAB-SIO10	10.2.4.40	00-27-0E-0F-86-79	LSO-010
LTG-LAB-SIO11	10.2.4.41	00-27-0E-0F-8A-A7	LSO-011
LTG-LAB-SIO12	10.2.4.42	00-27-0E-0F-74-D1	LSO-012
LTG-LAB-SIO13	10.2.4.43	00-27-0E-0F-8B-09	LSO-013
LTG-LAB-SIO14	10.2.4.44	00-27-0E-0F-8B-32	LSO-014
LTG-LAB-SIO15	10.2.4.45	00-27-0E-0F-74-62	LSO-015

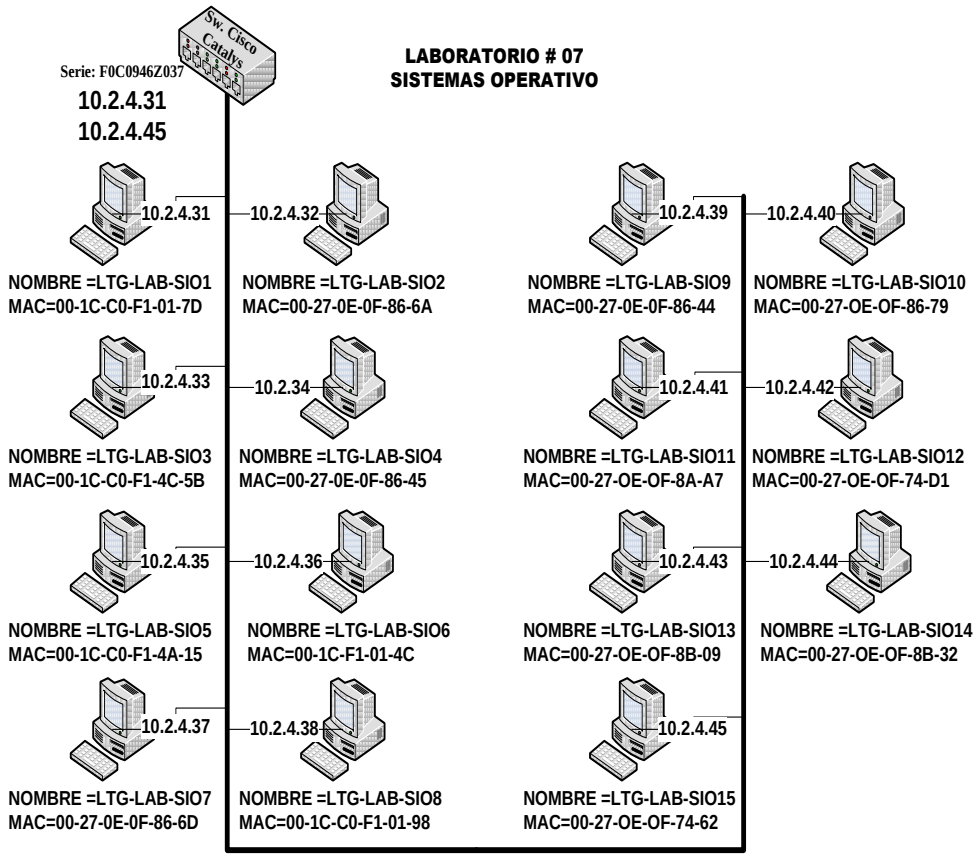


Figura 3.13. Red Física del Laboratorio N’07

LABORATORIO No 08 "INTELIGENCIA ARTIFICIAL"

Este laboratorio consta de 01Patch Panel, 01 Switch (Sw. 3Com Serie: 0300-LZ1V4NBD83340), y 16 Host. La interface al distribuidor principal es el puerto 08.

SOFTWARE INSTALADOS

Win Xp Sp3, Office 2007, Visual Basic 6.0, Winzip, Acrobat Reader 5.0

Tabla 3.12. Detalles de los Equipos del Laboratorio N'08

DETALLE DE LOS EQUIPOS			
NOMBRE DEL EQUIPO	**DIRECCION IP**	**DIRECCION MAC**	**NOMINATIVO**
LTG-LAB-ITA1	10.2.4.71	00-21-5A-E7-90-32	LIA-001
LTG-LAB-ITA2	10.2.4.72	00-21-5A-E7-06-FA	LIA-002
LTG-LAB-ITA3	10.2.4.73	00-21-5A-E7-97-48	LIA-003
LTG-LAB-ITA4	10.2.4.74	00-21-5A-E7-97-76	LIA-004
LTG-LAB-ITA5	10.2.4.75	00-21-5A-E7-97-CE	LIA-005
LTG-LAB-ITA6	10.2.4.76	00-21-5A-E7-90-50	LIA-006
LTG-LAB-ITA7	10.2.4.77	00-21-5A-E7-97-A8	LIA-007
LTG-LAB-ITA8	10.2.4.78	00-21-5A-E7-97-94	LIA-008
LTG-LAB-ITA9	10.2.4.79	00-21-5A-E7-90-9C	LIA-009
LTG-LAB-ITA10	10.2.4.80	00-21-5A-E7-97-35	LIA-010
LTG-LAB-ITA11	10.2.4.81	00-21-5A-E7-8E-F8	LIA-011
LTG-LAB-ITA12	10.2.4.82	00-21-5A-E7-97-92	LIA-012
LTG-LAB-ITA13	10.2.4.83	00-21-5A-E7-90-16	LIA-013
LTG-LAB-ITA14	10.2.4.84	00-21-5A-E7-90-1F	LIA-014
LTG-LAB-ITA15	10.2.4.85	00-21-5A-E7-97-87	LIA-015
LTG-LAB-ITA16	10.2.4.86	00-21-5A-E7-97-A5	LIA-016

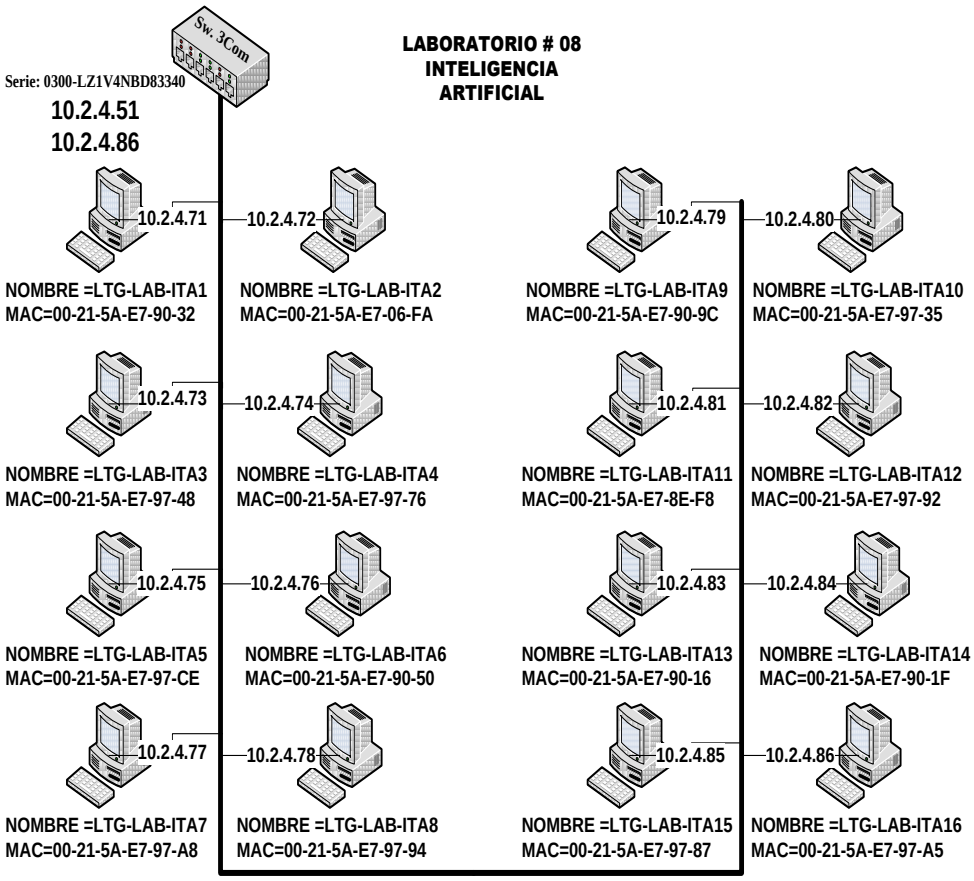


Figura 3.14. Red Física del Laboratorio N'08

LABORATORIO No 09 "COMPUTACIÓN III"

Este laboratorio consta de 01Patch Panel, 01 Switch (Sw. Cisco Catalys Serie: F0C0946Z03V), y 16 Host. La interface al distribuidor principal es el puerto 09.

SOFTWARE INSTALADOS

Win Xp Sp3, Office 2007, Visual Basic 6.0, Winzip, Acrobat Reader 5.0

Tabla 3.13. Detalles de los Equipos del Laboratorio N'09

DETALLE DE LOS EQUIPOS			
NOMBRE DEL EQUIPO	**DIRECCION IP**	**DIRECCION MAC**	**NOMINATIVO**
LTG-LAB-MIII1	10.2.4.191	00-21-5A-E7-97-8E	LC3-001

LTG-LAB-MIII2	10.2.4.192	00-21-5A-E7-97-9F	LC3-002
LTG-LAB-MIII3	10.2.4.193	00-21-5A-E7-90-3A	LC3-003
LTG-LAB-MIII4	10.2.4.194	00-21-5A-E7-90-85	LC3-004
LTG-LAB-MIII5	10.2.4.195	00-21-5A-E7-97-9B	LC3-005
LTG-LAB-MIII6	10.2.4.196	00-21-5A-E7-97-A2	LC3-006
LTG-LAB-MIII7	10.2.4.197	00-21-5A-E7-97-17	LC3-007
LTG-LAB-MIII8	10.2.4.198	00-21-5A-E7-90-90	LC3-008
LTG-LAB-MIII9	10.2.4.199	00-21-5A-E7-97-72	LC3-009
LTG-LAB-MIII10	10.2.4.200	00-21-5A-E7-90-44	LC3-010
LTG-LAB-MIII11	10.2.4.201	00-21-5A-E7-97-3D	LC3-011
LTG-LAB-MIII12	10.2.4.202	00-21-5A-E7-97-CA	LC3-012
LTG-LAB-MIII13	10.2.4.203	00-21-5A-E7-97-85	LC3-013
LTG-LAB-MIII14	10.2.4.204	00-21-5A-E7-97-C7	LC3-014
LTG-LAB-MIII15	10.2.4.205	00-21-5A-E7-90-4D	LC3-015
LTG-LAB-MIII16	10.2.4.206	00-21-5A-E7-90-99	LC3-016

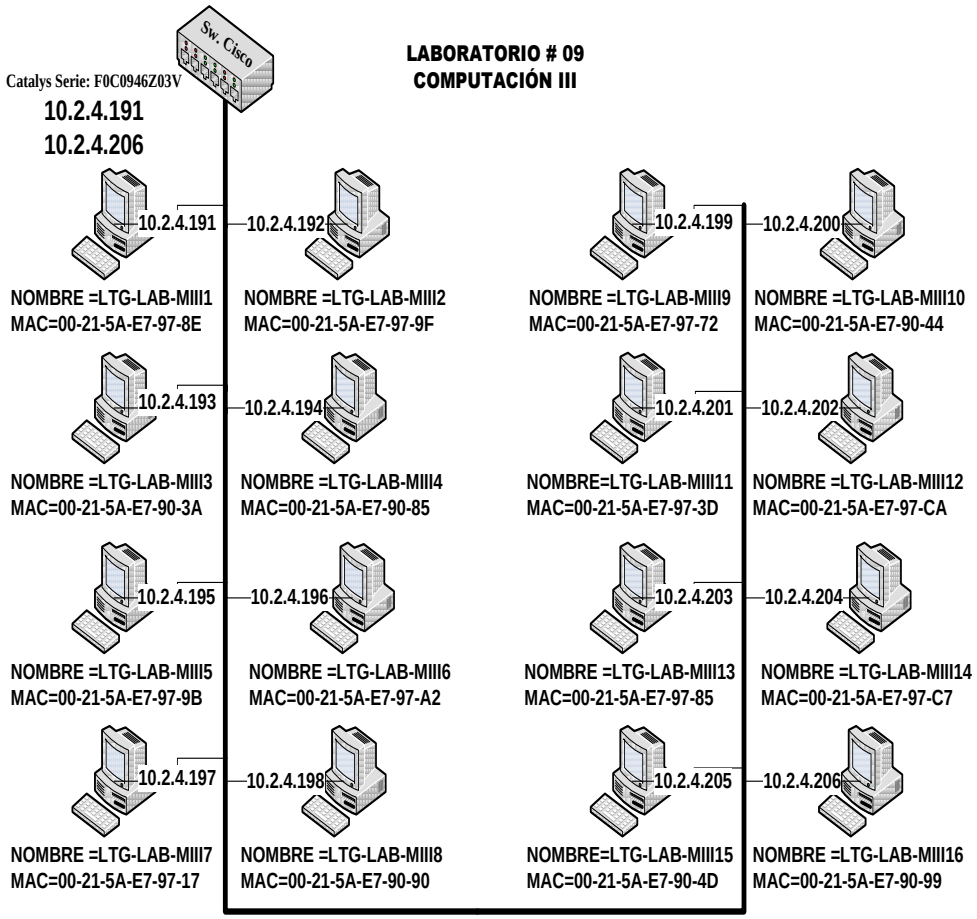
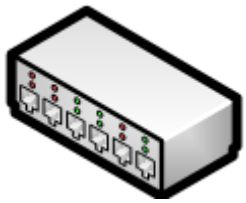


Figura 3.15. Red Física del Laboratorio N'09

3.3.2.7 CARACTERÍSTICAS TÉCNICAS DE LOS EQUIPOS DE INTERNETWORKING DEL LABORATORIO DE SISTEMAS PARA EL INTERNETWOWKING

A continuación se detalla las características de algunos equipos que dispone la red

3.3.2.7.1 SWITCH CISCO CATALYST 3550 24-10/100 2GBIC P



Descripción:

- IN Descripción del producto Cisco Catalyst 3550-24 EMI - conmutador - 24 puertos.
- Factor de forma Externo.
- 1 U Garantía del fabricante Garantía del tiempo de vida útil.
- Dimensiones (Ancho x Profundidad x Altura) 36.6 cm x 44.5 cm x 4.5 cm
- Peso 5 kg
- Alimentación CA 110/230 V CA 100/240 V (50/60 Hz)
- Memoria RAM 64 MB (instalados) / 64 MB (máx.)
- Tipo de dispositivo Conmutador
- Cantidad de puertos 24 x Ethernet 10Base-T, Ethernet 100Base-TX
- Velocidad de transferencia de datos 100 Mbps
- Protocolo de interconexión de datos Ethernet, Fast Ethernet
- Cumplimiento de normas IEEE 802.3, IEEE 802.3U, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.1w, IEEE 802.1x, IEEE 802.1s
- Modo comunicación Semidúplex, dúplex pleno
- Memoria Flash 16 MB (instalados) / 16 MB (máx.)

- Protocolo de gestión remota SNMP 1, SNMP 2, RMON 1, RMON 2, SNMP
- Encaminamiento IP, soporte de DHCP, negociación automática, soporte VLAN, activable, apilable Ranuras vacías 2 x GBIC.

3.3.2.7.2 SWITCH CISCO CATALYST 2950 24TT 24p

Características:

- Transmisión de datos
- Tasa de transferencia (máx) 0.1Gbit/s
- Full dúplex
- Velocidad de transferencia de datos 1000Mbit/s
- Capacidad de conmutación 16Gbit/s
- Tamaño de la tabla de direcciones 8000entries
- Características de red
- ACL, ARP, DiffServ, IGMP, IP, RADIUS, SSH, TCP, UDP, DHCP, TFTP
- Protocolos de gestión
- Telnet, RMON 2, RMON 1, SNMP 1, SNMP 3, SNMP 2c, TFTP, SSH
- Protocolo de trasmisión de datos Ethernet, Fast Ethernet
- Conectividad
- Cantidad de puertos 24
- Tecnología de conectividad Wired
- Puertos de entrada y salida (E/S) 24 x 10/100, 2 x 10/100/1000-TX
- Memoria Flash 32MB
- Peso y dimensiones Montaje en bastidor 1U
- Dimensiones (Ancho x Alto x Largo) 445 x 236 x 44mm
- Peso 3600g

- Emisión de sonidos Emisiones de presión acústica 40dB
- Gerencia de la energía
- Energía sobre Ethernet (PoE), soporte N
- Requisitos de energía 100-240VAC, 1.3-0.8A, 50-60 Hz
- Requisitos del sistema
- Memoria interna, mínimo (RAM) 64MB
- Resistencia Tiempo medio entre fallos 282,416h
- Aprobaciones reguladoras
- Cumplimiento de estándares del mercado
- IEEE 802.1d, IEEE 802.1p, IEEE 802.1Q, IEEE 802.3 CSMA/CD, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3z, IEEE 802.1w, IEEE 802.3x, IEEE 802.1x, IEEE 802.1s
- Seguridad
- UL, C-UL, TUV/GS, CB, NOM, CE
- Condiciones ambientales
- Altitud operacional 3049m
- Humedad relativa 10-85%
- Temperatura -25-70°C
- Alcance de temperatura operativa 0 - 45°C
- Altitud no operativa 4573m
- Iluminación/Alarmar Indicadores LED

3.3.2.7.3 3Com 3C17304 SUPERSTACK3 4228G 24Port 10/100 + 2 10/100/1000 + 2 empty GBIC Ports – New

Descripción:

- El SuperStack 3 Switch 4228G es un switch LAN de 28-port 10/100 LAN para requerimientos de red de última tecnología.
- Con 24 puertos 10/100, dos puertos Gigabit de cobre para stacking o downlinks, y dos slots GBIC adicionales para conexiones Gigabit.

- Ofrece características de capa 2 incluyendo rendimiento de wirespeed, 802.3ad Link Aggregation (LACP) en enlaces Giga bit, Rápido Spanning Tree Protocol, y soporte de Advanced Redundant Power Supply.
- GBIC's soporta conexiones de fibra y cobre.
- Stack con otros Switch 4200 hasta cuatro unidades, sin hardware adicional. Soporta Auto-negociación, auto MDI/MDIX, y DHCP.

3.3.2.7.4 HP ProCurve Switch 2524

Descripción:

- Switch gestionable, apilable y económico que proporciona 24 puertos 10/100Base-TX Autosensing, HP Auto-MDIX en todos los puertos 10/100 y 100/1000, características de alta disponibilidad y 2 slots para transceptor Gigabit o 100Base-FX.
- Disfruta del más elevado rendimiento en 10/100 y Gigabit, gracias al backplane de 9.6 Gbps, y la mejor fiabilidad, dado el diseño "en un chip".
- Estos switches se presentan en configuraciones apilables, con detección automática del tipo de cable en todos los puertos MDI/MDI-X y dos slots libres para transceptor Gigabit o 100FX.
- Estos HP Procurve switch son idóneos para realizar una migración económica a la conmutación gestionable 10/100 con enlaces ascendentes.
- Tienen gestión SNMP, RMON y RMON Extendido, Trunking LACP (802.3ad), VLAN, GVRP, IGMP, Spanning Tree, CoS 802.1p, TACACS+, 802.1x y RADIUS. Cuentan con gestión basada en Web y software HP TopTools para Hubs y Switches.

- Este modelo presenta 24 puertos RJ-45 10/100Base-TX (IEEE 802.3 tipo 10Base-T; 802.3u tipo 100Base-TX) Autosensing, dos slots libres para transceptor y un puerto de consola DB-9 RS-232C.
- El tamaño de la memoria intermedia de paquetes es de 6 MB compartidos por las memorias intermedias de paquetes. La capacidad de la RAM/ROM es de 26 MB. El procesador es del tipo ARM7TDMI con una velociada a 62.5 MHz. La capacidad flash es de 2 MB.
- La matriz de conmutación de 9.6 Gbps integrada en el chip proporciona un diseño de switch de alto rendimiento con arquitectura sin bloqueo. Tiene un gran rendimiento sin mas de 10 µs (LIFO) de latencia y una capacidad para 6.6 millones de pps (paquetes de 64 bytes).
- El HP Auto-MDIX ajusta automáticamente el switch para utilizar cables de conexión directa o de cruce en todos los puertos 10/100 y 100/1000.
- Al ser apilable permite la gestión de una única dirección IP para una pila virtual de hasta 16 switches, incluidos los modelos 1600m, 2400m, 2424m, 2512, 2524, 4000m y 8000m.
- Cuenta con RMON y RMON extendido que proporcionan posibilidades avanzadas de monitorización.
- La interface de Web permite configurar el switch desde cualquier navegador de Web de la red.
- El enlace estándar IEEE 802.3ad permite combinar conexiones redundantes entre dispositivos para obtener un mayor ancho de banda total entre dispositivos que admitan LACP (Link Aggregation Control Protocol).
- Admite VLANs y etiquetado de VLAN, admite hasta 30 VLANs basadas en puertos y la configuración dinámica del etiquetado VLAN 802.1Q para aportar seguridad entre grupos de trabajo.

- El Group VLAN Registration Protocol (GVRP) permite memorizar automáticamente las VLANs, eliminando la necesidad de configurarlas manualmente.
- IP multicast (IGMP) impide la inundación del tráfico en IP multicast.
- La seguridad de los puertos mantiene la seguridad de la red y de los usuarios, impidiendo su manipulación por parte de usuarios no autorizados.
- El Protocolo Spanning Tree proporciona enlaces redundantes al tiempo que impide bucles en la red.
- La asignación de prioridades IEEE 802.1p entrega datos a los dispositivos en función de la prioridad y el tipo de tráfico.
- TACACS+ facilita la administración de la seguridad del switch utilizando un servidor de autentificación de contraseñas.
- El acceso a la red basado en 802.1x y RADIUS controla el acceso y proporciona autentificación y responsabilidad para la seguridad de la red Cisco Fast Ether Channel proporciona mayor capacidad con otros dispositivos que admitan FEC.
- Se monta en un bastidor estándar de 19" con elementos de fijación incluidos.

3.3.2.7.5 HUB D-LINK DSH-16 10/100 16 PUERTOS

Descripción:

- **10/100**
- 2 uplink,
- **16 PUERTOS**
- Funcionando impeke.

3.3.2.7.6 SERVIDOR POWER EDGE 4600

Arquitectura

- Factor de forma: Torre
- Orientación: Vertical
- Tipo de bus / Arquitectura: PCI-X
- Procesador (unidad central de proceso): Intel Xeon
- Velocidad interna del procesador: >= 3.06 Ghz
- Velocidad del bus del sistema: >= 533 Mhz
- Capacidad de multiprocesamiento simétrico: >=2
- CACHE de nivel 2: >=512 KB por procesador
- Tipo de BIOS: Flash
- Configuración inicial: Al menos hasta dos procesadores
- Memoria RAM
- Capacidad: >= 2GB (dos módulos de 1GB)
- Velocidad: >= 533 Mhz(acorde a la velocidad del bus)
- Tipo de RAM: ECC DDR SDRAM ó mejor
- Número de slots: >= 6
- Configuración inicial: Al menos hasta 6GB
- NOTA: El número de slots puede ser menor si la configuración compensa (Ej. 6 Slots y soporte de DIMMs de 2 GB)
- Controlador SCSI RAID para almacenamiento físico PCI-X ó mejor.
- Dos canales Ultra 320 SCSIAl menos 64 MB de cache ó mejor soportado con batería.
- Soporte para arreglo RAID 0, 1, 5, 5e y 10Soporte para expansión de arreglos

- Networking: Tarjeta interfase de red: 5 Interfaces RJ45 Ethernet 10/100/1000 Mbps Full duplex, Diseñadas para servidor.
- Bahías para dispositivos
- Bahías 3.5" accesibles desde el frente:3 SL, una para el disco flexible y 2 de intercambio en caliente para discos duros Ultra320 SCSI o mejor.
- Bahías 5.25" accesibles desde el frente: 2 HH, para unidad de CD/DVD-ROM, unidad de backup, etc.
- Almacenamiento interno
- Discos duros soportados: Intercambio en caliente Ultra 320 SCSI, 18GB, 36GB y 73GB a 10K rpm y 15K rpm o mejor
- Configuración inicial: Al menos 2 discos duros Ultra320 SCSI de 36 GB y 10K rpm en arreglo RAID 1
- Opciones de expansión
- Slots/tipo: 2 PCI-X de tamaño completo 64bits/133 Mhz o mejor
- Interfaces: Puertos Ethernet RJ-45, serial, paralelo, teclado, mouse, gráfico (video) y SCSI externo
- Subsistema gráfico
- Tipo: SVGA
- Tipo de video RAM: SGRAM
- Capacidad de video RAM: 8 MB
- Resolución: 1024x768 a 75 hz y 65536 colores o mejor
- Configuración inicial: 8 MB de RAM de video
- Características multimedia
- Velocidad de CD/DVD-ROM: 24 X ó mejor
- Tipo de interface de CD/DVD-ROM SCSI/IDE
- Almacenamiento removible
- Disco flexible: 3.5" 1.44 MB
- Unidad de respaldo SCSI interna 20/40 GB
- Administración de poder

- Fuentes de poder: Estándares y redundantes
- Ventiladores: Estándares y redundantes
- Característica de administración de poder:
- Reinicio automático
- Emisión de ruido: Baja
- Compatibilidad del Hardware: Todo el hardware debe ser compatible con: Sistemas operativos: Linux >=2.4, FreeBSD >= 4.6, Windows NT Server 4.0, Windows 2003 Server, Windows 200 Server, Solaris.
- Software
- Sistema operativo Linux RedHat Server E. Ultima versión

3.3.2.7 PROPUESTAS DE MEJORAS

1. Los usuarios pueden ser parte de muchos grupos de trabajo y pueden ejecutar muchas aplicaciones, los switches capa 4 proporcionan una tabla de filtraje mucho más grande que un switch capa 3 o capa 2. Por todo esto, se necesita de un switch capa 4 en el núcleo (core) del modelo jerárquico para óptimo funcionamiento de la red de la ESPEL.
2. La disposición de los paneles, organizadores y equipos en el rack no es la más adecuada. Usualmente deberían ubicarse los organizadores horizontales entre paneles y equipos de modo de ayudar en la administración de la interconexión de los cordones de conexión (patch cords). Muestra un crecimiento no planificado.
3. La red Wireless actualmente se encuentra en el área académica, ésta debería tener un acceso aparte, para que se maneja usando otro rango como una red independiente.
4. El diseño óptimo de la Red de datos de la ESPE-L implica realizar algunos cambios en equipos; el incremento de otros y la reasignación de nuevas direcciones.
5. Ante la tendencia actual de todas las Universidades de disponer de tecnología de punta, con aplicaciones que reduzcan los costos de

algunos servicios, como es la telefonía, se debería implementar en la intranet de la ESPE-L, el servicio de VoIP en todas las áreas.

6. El sistema de acondicionamiento ambiental se debería implementar en el Centro de Datos 1, para de esta manera realizar una protección a los equipos de la red como son los servidores que dispone la ESPEL.
7. Deberán implementarse nuevas políticas de seguridad, de acuerdo a un plan establecido por la Unidad de las TIC´s y socializado por todos los usuarios de la Red.
8. Es muy recomendable para el administrador de la red entregar una copia con las medidas de seguridad básicas o la política del sistema, a cada usuario al crear su cuenta.

3.4 SEGURIDAD DE LA RED DE DATOS

La seguridad es un estado del bienestar de la información y de las infraestructura en el cual la posibilidad de hurto, de tratar de forzar, y de interrupción de la información y de los servicios se han mantenido en un punto bajo o tolerante.

Existen varios aspectos que tiene que ver con la seguridad en la actualidad; el dueño de un sistema deberá tener la confianza que el sistema se comportara según su especificación. A esto se le llama generalmente aseguramientos, los sistemas, usuarios, y aplicaciones necesitan interactuar recíprocamente uno con otro en un ambiente de trabajo en red. La identificación o la autenticación es el medio para garantizar la seguridad en tal panorama. Los administradores de sistema o cualquier otra autoridad necesitan saber quien ha tenido acceso a los recursos del sistema cuando, donde, y para que propósito, una auditoria a los losg (registro diario) puede tratar el aspecto de la seguridad llamado manejo de cuentas. No todos los recursos estarán generalmente disponibles para todos los usuarios. Esto puede tener implicaciones estratégicas; ya que teniendo controles de

acceso en parámetros predefinidos puede ayudar a alcanzar un mejoramiento en la seguridad.

3.4.1 PLANEACIÓN DE LA SEGURIDAD EN LA RED

El activo más importante que se posee es la información, y por lo tanto deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacenan. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y solo permiten acceder a ellos a las personas autorizadas para hacerlo. En la seguridad lógica debe tomarse en cuenta lo que es bien conocido dentro de la seguridad informática: "lo que no está permitido debe estar prohibido"

3.4.2 MODELOS DE LA SEGURIDAD

Los modelos de la seguridad en la red permiten definir la forma en la que se protegerá principalmente la información que se encuentra dentro de una red.

Cabe mencionar que ningún modelo garantiza la seguridad total de un sistema; es decir los modelos pueden fallar.

3.4.2.1 Seguridad por oscuridad

Este modelo consiste en los sistemas no son protegidos porque sus propietarios creen que nadie los va atacar porque no les interesa, piensan que la probabilidad de que les ataquen es ínfima, por lo tanto, no hacen nada por mejorar su estado actual; es decir, no conocen sus vulnerabilidades y pueden ser atacados.

3.4.2.2 Perímetro de defensa

Este modelo establece un cerco o perímetro de defensa externa, para que posibles atacantes externos no tengan acceso a los sistemas. Este modelo

es vulnerable a usuarios a atacantes internos, debido a que internamente se puede tener acceso a la información si restricciones de ningún tipo.

También tiene sus falencia, dado que los sistemas de seguridad externos utilizados son subsistidles, dejando de esta manera la red desprotegida.

3.4.2.3 Defensa de profundidad

Este modelo es el efecto de ir acortando los perímetros de defensa, puede diferenciar servidores de usuarios para establecer seguridad, establecer varios perímetros de seguridad, donde cada perímetro se reduce hasta un nivel en el cual cada uno de los sistemas sea una isla o perímetro seguro.

Como contraparte, la administración de este modelo de seguridad resulta bastante compleja y costosa pues se debe asegurar cada uno de los elementos de un sistema teniendo en cuenta sus características y funcionamiento.

3.4.3 Servicios implícitos en la seguridad en Red

La seguridad en redes por definición brinda servicios que permiten a la información y a los recursos estar disponibles a los usuarios de la organización y protegidos contra intentos de acceso no consentidos. A continuación se detallaran los principales servicios y sus funciones.

3.4.3.1 Confidencialidad

Este servicio permite mantener la privacidad de la información; es decir, solo usuarios autorizados pueden tener acceso a la información y entenderla. Para conseguir esto, la información que se desea proteger es cifrar; por consiguiente, si u intruso tiene acceso a la información no podrá entender su contenido.

3.4.3.2 Integridad

Este servicio garantiza que la información llegara a su destino durante el tiempo previsto y sin alteraciones. Para este propósito, el emisor obtiene un resumen de la información enviada y adjunta este resumen a la información. En el destino la información es separada del resumen y el procedimiento se repite para obtener un nuevo resumen y poder comparar los dos resúmenes, si coinciden, se puede confiar en el contenido de la información.

3.4.3.3 Disponibilidad

La disponibilidad esta dad por el tiempo que un sistema permanece en línea con respecto al tiempo que estará fuera de servicio, se mide en porcentaje.

Para exista la disponibilidad hardware y software deben ser confiables; la disponibilidad siempre se ajustara a los requerimientos de una empresa especifica, dado que para cumplir con este servicio se deberá disponer de redundancia ya sea en sistemas o canales de comunicación.

3.4.3.4 Identificación

Es el proceso mediante el cual se establece la identidad de un individuo en particular. Se puede identificar a personas o entidades, para esto se lleva a cabo procedimientos que garanticen que la identidad presentadas corresponda a la entidad. Por ejemplo, se puede requerir a la presentación de una cedula de identidad personal, pasaporte, fotografías, dirección, teléfono e incluso referencias personales.

3.4.3.5 Autenticación

Es un proceso que consiste en presentar una prueba de ser quien se dice ser, es muy importante cuando se ingresa o se comunica de una red.

Para la autenticación se utiliza tres esquemas básicos:

- Algo que usted conoce: password o contraseña
- Algo que usted tiene: tarjeta o llave
- Algo que usted es: iris del ojo humano, huella dactilar, voz.

Estos esquemas generalmente son utilizados independientemente, aunque se recomienda que se usen en dos conjunto.

3.4.3.6 Control de Acceso

Este servicio consiste en autorizar a usuarios lícitos el acceso a recursos e información de acuerdo a su función. Cada función de un usuario está definida en un perfil que determina que está permitido y que no lo está.

3.4.3.7 Aceptación (para impedir a la negación de eventos)

Este servicio permite garantizar que usuarios lícitos no pueden realizar acciones ilícitas, como realizar una transacción y después negarla. Para que este servicio sea garantizado se necesita integrar en los mensajes un registro del tiempo en que fueron enviados y recibidos.

3.5 INSTALACIÓN DE LANGUARD NETWORK SECURITY SCANNER

3.5.1 Requerimientos del sistema

- Sistema operativo Windows 2000 (SP4)/ XP (SP2)/ 2003, Windows 7.
- Internet Explorer 5.1 o superior.
- Componente Cliente para Redes Microsoft - (incluido por defecto en Windows 95 o superior)

3.5.2 Procedimiento de instalación.

1. Hacer doble clic en languardnss7.exe., luego clic en Next para iniciar la instalación.(Ver Figura 3.16)

Figura 3.16. Inicio de software

2. En el diálogo de licencia, lea el acuerdo de licencia atentamente. Seleccione la opción 'Accept the Licensing agreement' y haga clic en Next para continuar.(ver Figura 3.17)

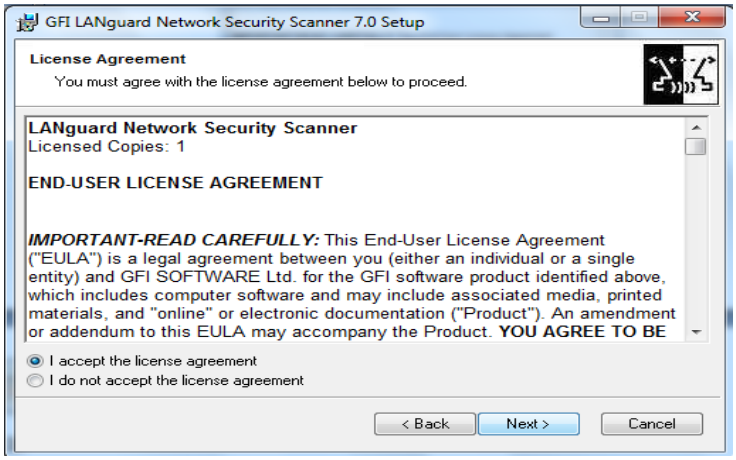


Figura 3.17 Aceptación de licencia

3. Especifique el nombre de usuario completo, el nombre de la empresa y la clave de licencia. Haga clic en Next para continuar. (ver Figura 3.18)

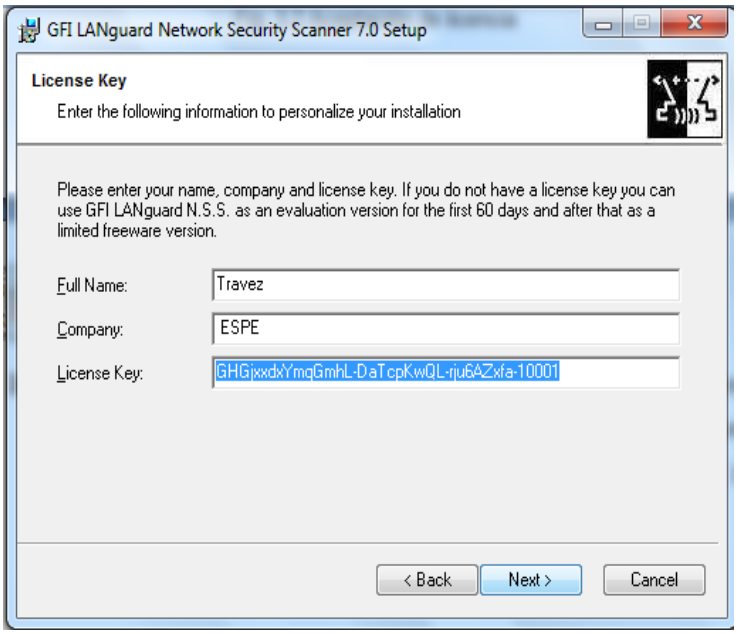


Figura 3.18 Especificar usuario, compañía, y licencia del software

4. Seleccionamos el tipo de perfil que deseamos instalar en este caso seleccionamos el primero. Y en el cuadro de dialogo clic en SI. Haga click en Next para continuar. (ver Figura 3.19 y 3.20)

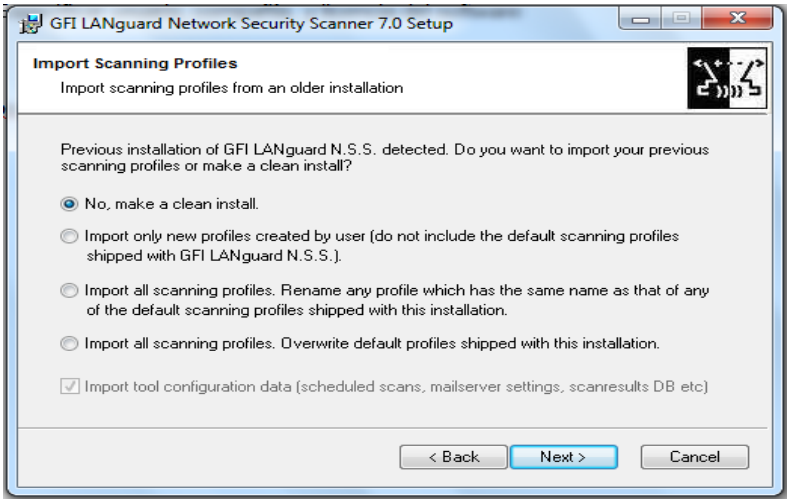


Figura 3.19 Instalación limpia

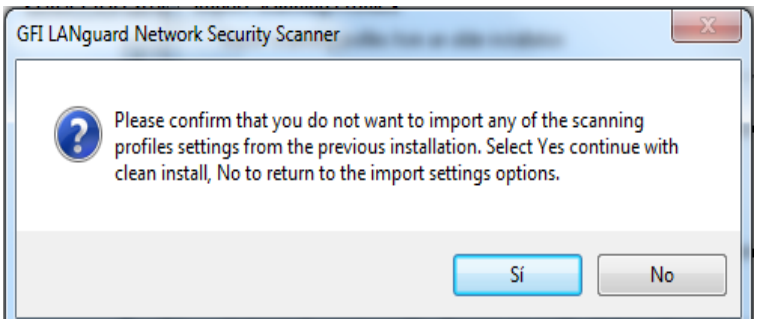


Figura 3.20 Mensaje de comprobación.

5. Especifique la cuenta de servicio bajo la cual correrá GFI LANguard. Haga clic en Next para continuar. (ver Figura 3.21)

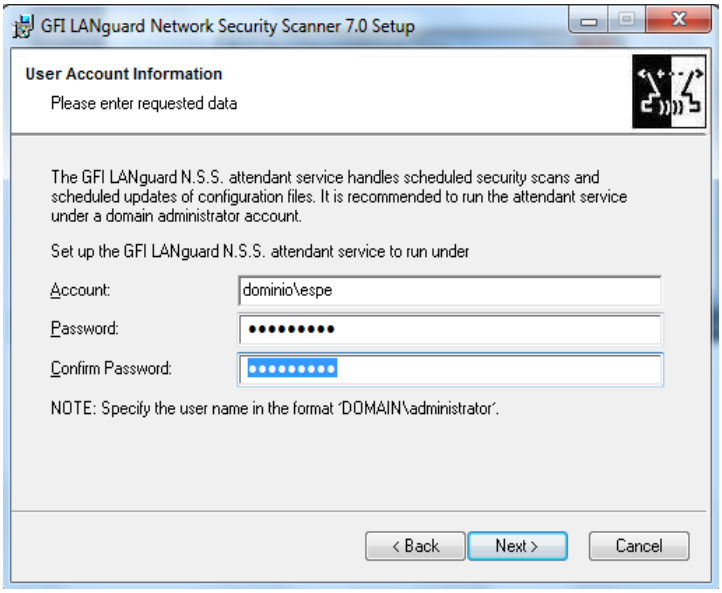


Figura 3.21. Especifique las credenciales del administrador.

6. Especifique que base de datos de respaldo se usará para almacenar los resultados e información del análisis. Puede elegir entre Microsoft Access, Microsoft SQL Server 7/2000 o MSDE. Haga clic en Next para continuar. (ver Figura 3.22)

Nota:

- Microsoft Access se recomienda para redes pequeñas
- Microsoft SQL Server es capaz de manejar grandes volúmenes de datos eficientemente y sin limitaciones.

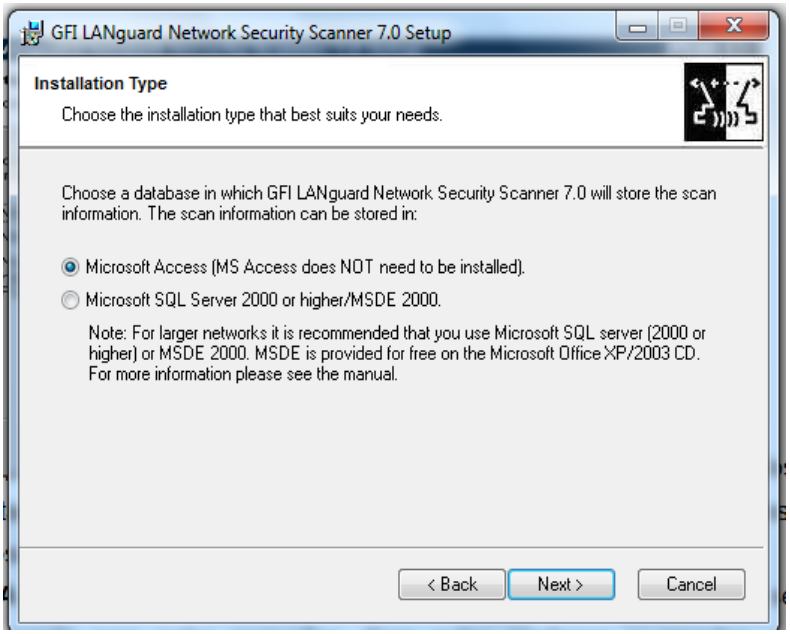


Figura 3.22 Elegir la base de datos de respaldo.

7. Si se selecciona Microsoft SQL Server como base de datos de respaldo, especifique las credenciales de inicio que se usarán para logarse en la base de datos.
8. Especifique la ruta de instalación de GFI LANguard N.S.S. y haga clic en Next. La instalación necesitará aproximadamente 40 MB de espacio libre en disco. (ver Figura 3.23)

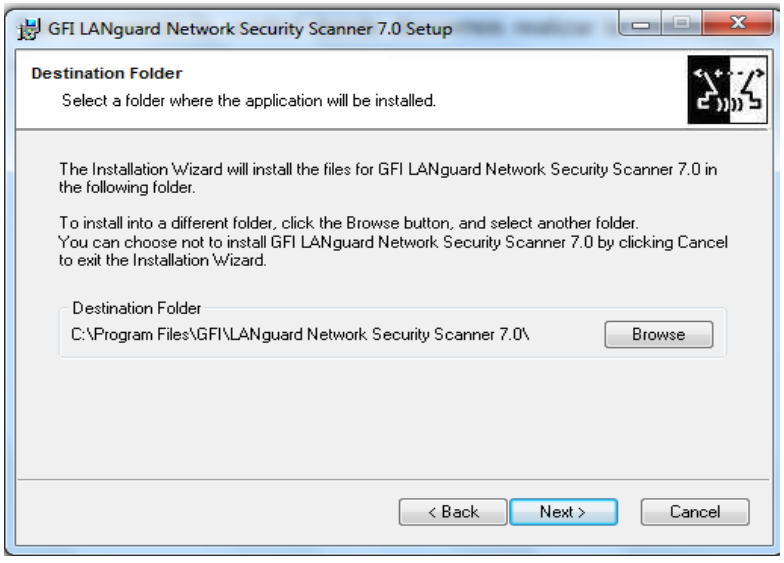


Figura 3.23 Elegir la unidad donde se guarda el software instalado.

9. Especifique la versión del software y el idioma. Haga clic en Next para continuar. (ver Figura 3.24)

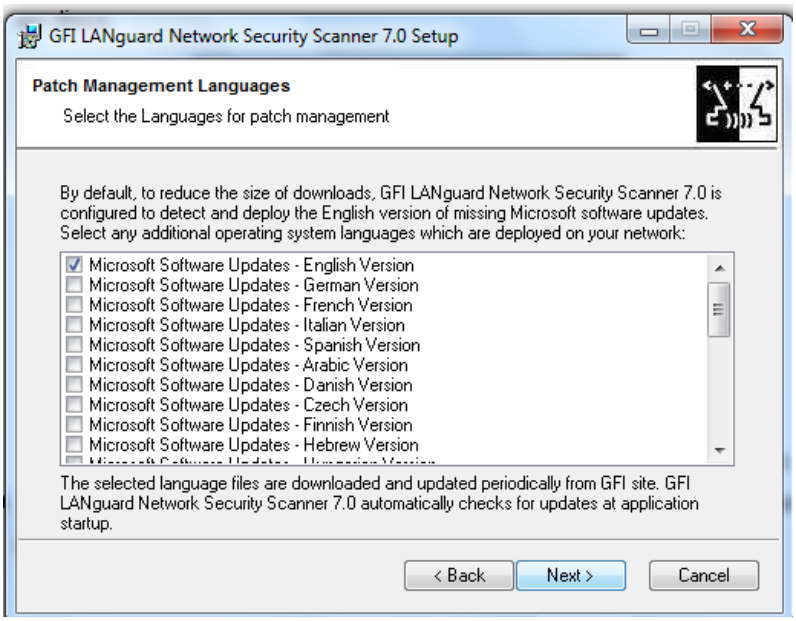


Figura 3.24 Especificar los detalles del servidor SQL.

10. Cuadro de mensaje listo para instalar la aplicación, haga clic en Next para continuar. (ver Figura 3.25)

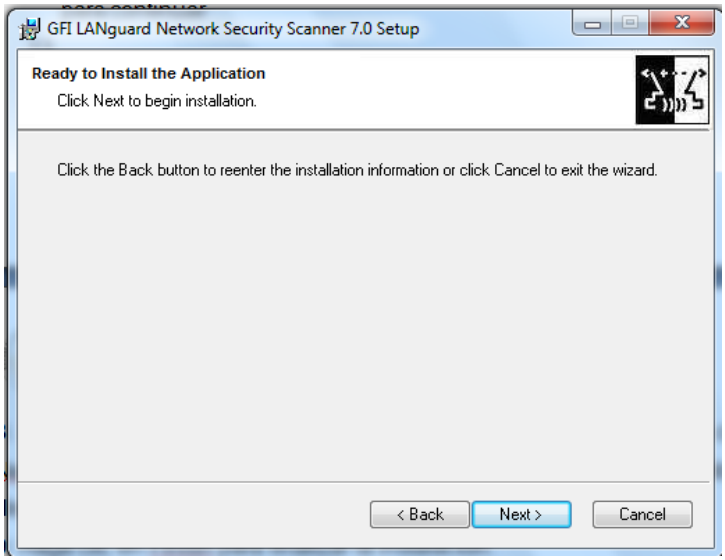


Figura 3.25. Listo para instalar la aplicación.

11. Haga clic en Finish para finalizar la instalación (ver Figura 3.26)

Figura 3.26 Finalizar la instalación

CAPÍTULO 4

ELABORACIÓN DEL MANUAL Y PRESENTACIÓN DE RESULTADOS

4.1.1 DEFINICIÓN Y FUNCIÓN DEL MANUAL

Este manual es una carpeta que abarca la información de los elementos básicos en el sistema de red, el objetivo es delimitar por escrito los parámetros y lineamientos a seguir para lograr controlar amenazas dentro de un área red, aclarando de antemano cualquier posible duda sobre los procedimientos de aplicación en los diferentes puntos instalados.

A continuación listamos las ventajas al utilizar el software de scaneo:

- Escáner de puertos, permitiendo al administrador localizar servicios no autorizados y potencialmente peligrosos que estén iniciados en la red.
- Detecta aplicaciones no autorizadas instaladas en la red y alerta inmediatamente al administrador.
- Chequea que las instalaciones de anti-virus estén actualizadas y asegura que las aplicaciones de seguridad funcionen correctamente.
- Detección y reportes de aplicaciones instaladas.

4.1.2 FASE DE APLICACIÓN Y CONTROL.

El administrador es el encargado de la puesta en marcha el manual que contiene los datos del software instalados así como la información necesaria de los laboratorios informáticos.

4.1.3 ELABORACIÓN DEL MANUAL.

Debido a la gran variedad de equipos y aplicaciones de red a las que enfrenta los Laboratorios informáticos nuestro objetivo constituye la elaboración de un manual, que se caracteriza por ser útil para los administradores que podrán identificar las causas que limitan la red y que

es necesario la instalación de un software GFI Languard Network Security Scanner, que está constituida por varios mecanismos para tener un control total de los problemas que puede ocasionar en cualquier momento no deseado.

4.1.4. PASOS PARA EL MONITOREO Y ESCANEO DE LA RED

Abrir en la máquina el programa (Inicio, Todo los programas, GFI LANguard Network Security Scanner, LANguard Network Security Scanner) donde aparecerá esta ventana listo para poder escanear escogiendo cualquiera de las opciones existentes (ver figura 4.1 y 4.2)

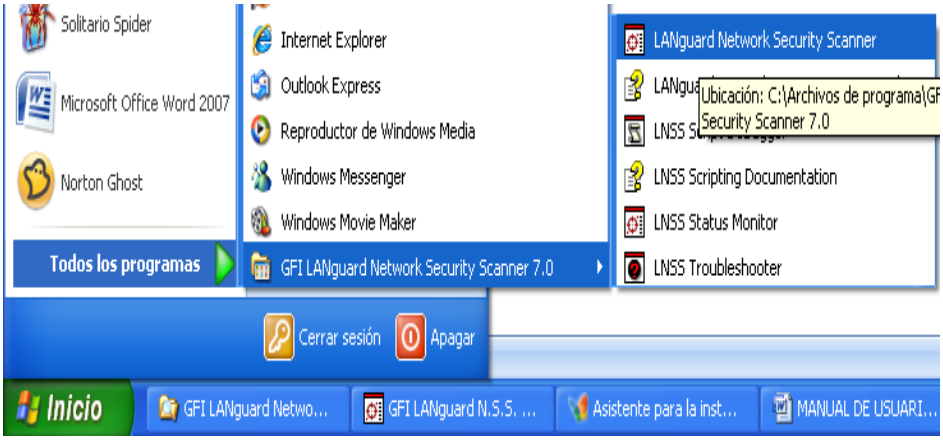


Figura 4.1Inicio del programa

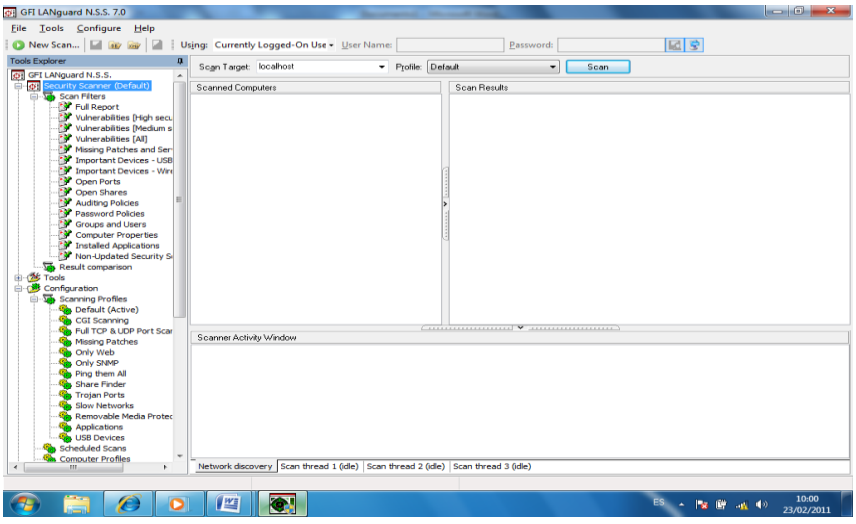


Figura 4.2 primera pantalla del Software

a. Hacer click en file, new y escoger la opción a realizar (ver figura 4. 3)

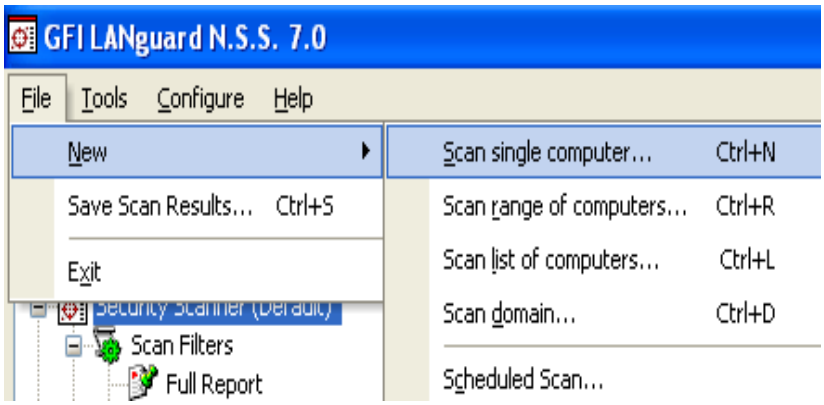


Figura 4.3 opciones para escanear

- **Scan single computer.-** Seleccionar esta opción para analizar un solo ordenador.
- **Scan range of Computers.-** Seleccionar esta opción para analizar un rango de ordenadores específico.
- **Scan list of Computer.-** Seleccionar esta opción para analizar una lista de ordenadores personalizada.
- **Scan a Domain.-** Seleccionar esta opción para analizar un dominio de Windows completo.
- **Scheduled Scan**. Esta opción se utiliza para configurar análisis de vulnerabilidad.

b. Hacer clic en el botón OK para iniciar su análisis por defecto (ver figura 4.4)

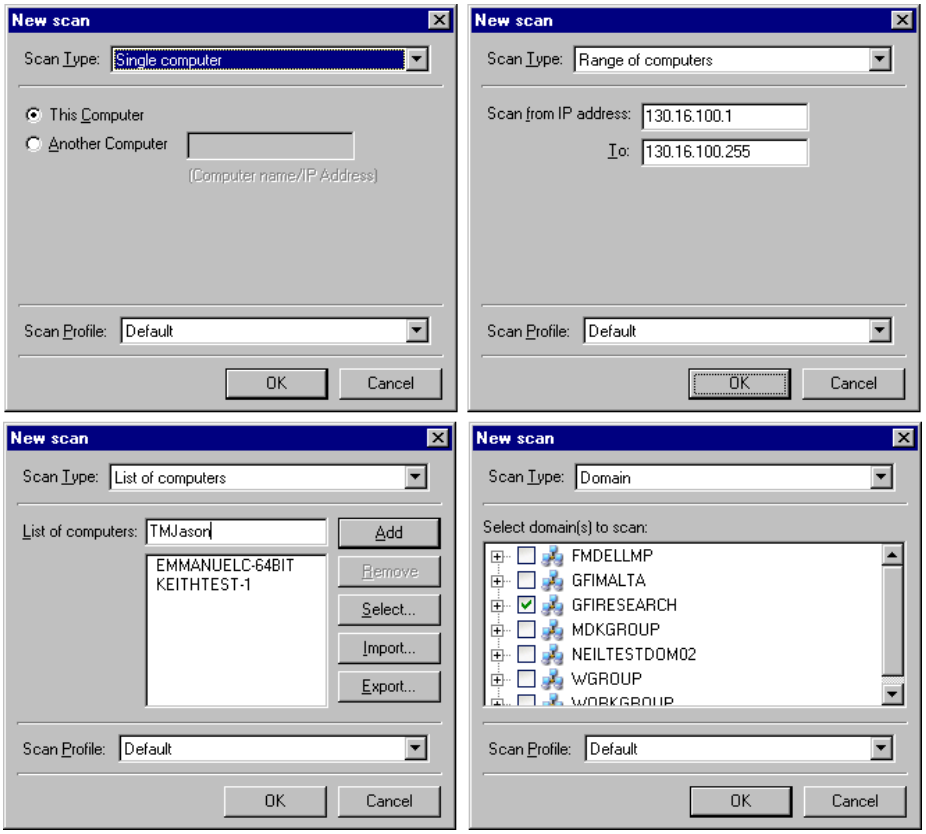


Figura 4.4 Opciones seleccionados

4.1.5 RESULTADOS DEL ANÁLISIS DE SEGURIDAD

Después de completar un análisis de seguridad, GFI LANguard genera y muestra los resultados del análisis en una ventana dedicada dentro del interfaz de configuración. Los resultados del análisis están organizados por tipo en diferentes categorías. La cantidad de categorías de resultados y el tipo de información recogida durante un análisis de seguridad depende enteramente del tipo de comprobaciones que han sido lanzadas contra los objetivos así como también de los parámetros que han sido configurados en el perfil de análisis que se ha usado durante la auditoría. Por lo tanto, se obtendrá por supuesto diferentes categorías de resultados del análisis por cada perfil de análisis diferente que utilice para auditar la red. (Ver figura 4.5)

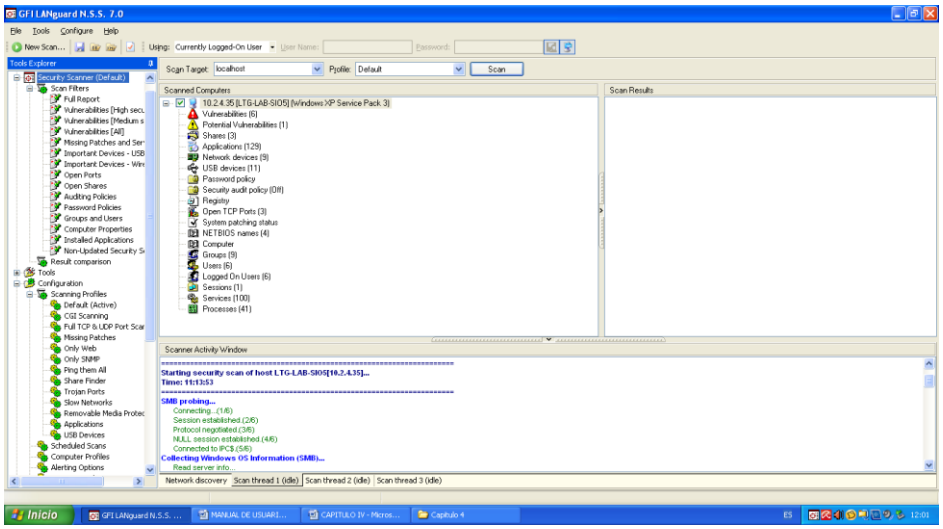


Figura 4.5 Categorías del escaneo

Utilizar la información presentada en la sección 'Scanned computers' (panel del medio) para navegar por los resultados de los ordenadores analizados.

Los resultados del análisis de seguridad están organizados en un número de sub-nodos de categoría. Esto puede ser fácilmente usado para investigar e identificar los problemas de seguridad en los objetivos analizados.

Los resultados del análisis están organizados en las siguientes categorías:

1. IP, nombre del equipo y sistema operativo
2. Vulnerabilidades
3. Potencial Vulnerabilidades
4. Shares
5. Aplicación
6. Network devices
7. USB devices
8. Password policy
9. Registry
10. Open TCP Ports
11. Netbios names

12. Computer
13. Groups
14. Users
15. Loggd On Users
16. Sessions
17. Services
18. Processes

Para ver los datos de los resultados de análisis recogidos durante un análisis de seguridad, hacer clic en la categoría de interés. La información se muestra en el panel 'Scan Results' (a la derecha).

1. Identifica la IP de una maquina escaneado, el nombre de un Laboratorio y el Sistema Operativo. (Ver la figura 4.6)

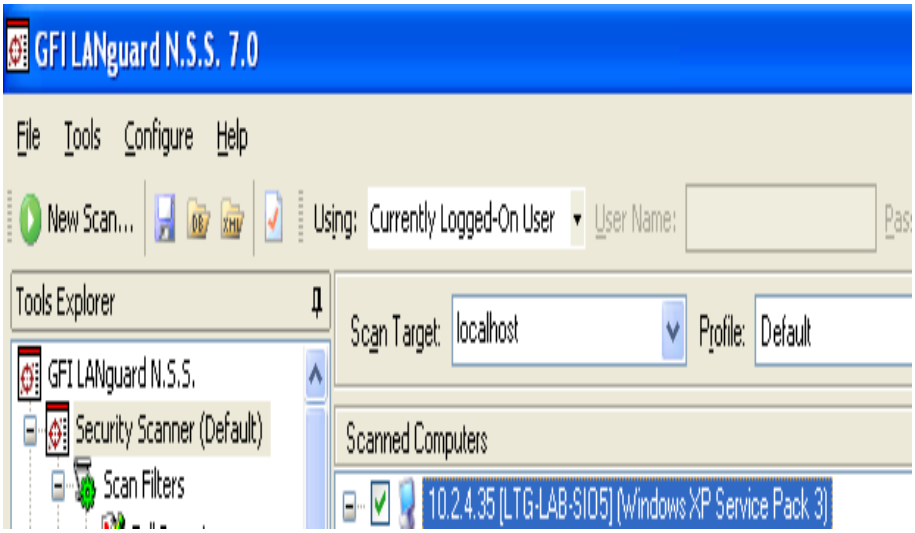


Figura 4.6 Nodo de la IP asignada.

2. Vulnerabilidades:

Hacer clic en el sub-nodo Vulnerabilities para ver las vulnerabilidades de seguridad identificadas en el equipo. Ver (Fig. 4.7)

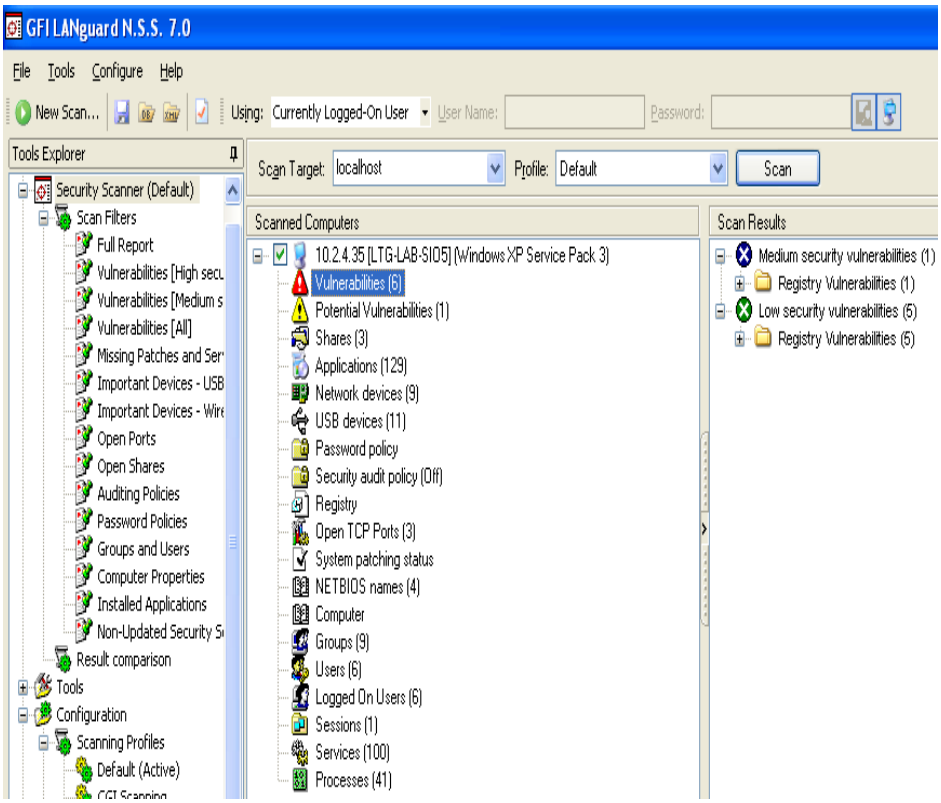


Figura. 4.7 Nodo de la vulnerabilidad.

3. Potencial Vulnerabilidades:

Hacer clic en el sub-nodo Potencial vulnerabilities para ver los elementos del análisis de resultados que son clasificados como posibles debilidades de red. Estos elementos del resultado de análisis, a pesar de que no están clasificados como vulnerabilidades, requieren su minuciosa atención dado que pueden ser explotados durante un ataque por usuarios malintencionados. (Ver Figura 4.8)

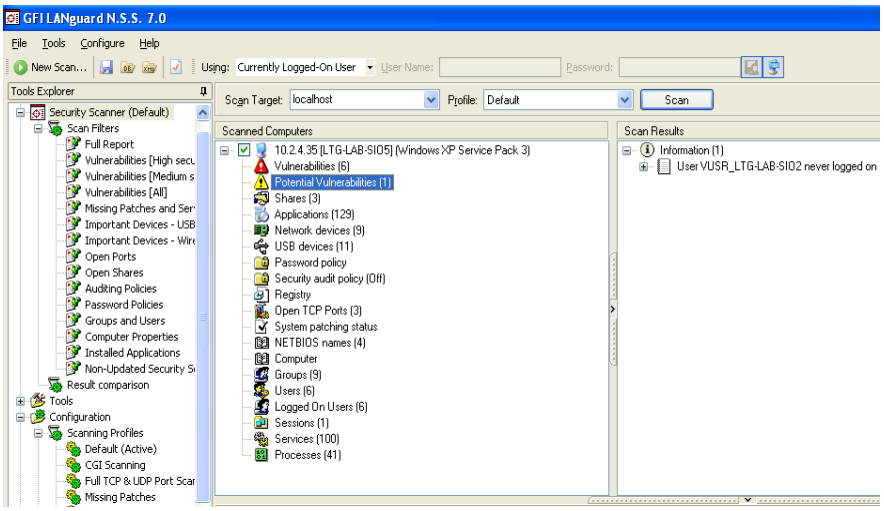


Figura 4.8 Nodo de las vulnerabilidades potenciales

4. Shares:

Hacer clic en el sub-nodo Shares para ver todos los recursos compartidos en un ordenador objetivo. (Ver Figura 4.9)

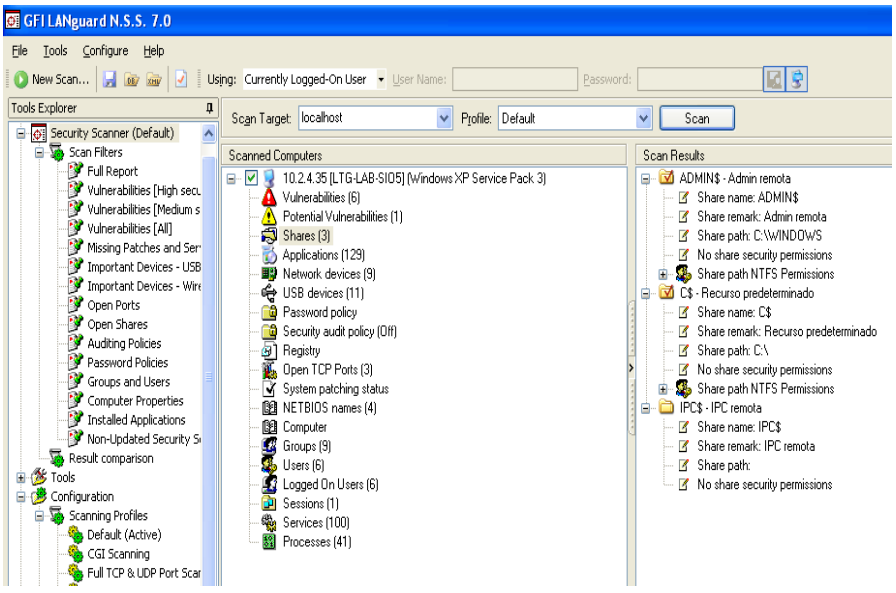


Figura 4.9 Nodo de Shares

5. Aplicaciones:

Hacer clic sobre el sub-nodo Applications para acceder a la lista completa de aplicaciones que están instaladas en un ordenador analizado. (Ver Figura 4.10)

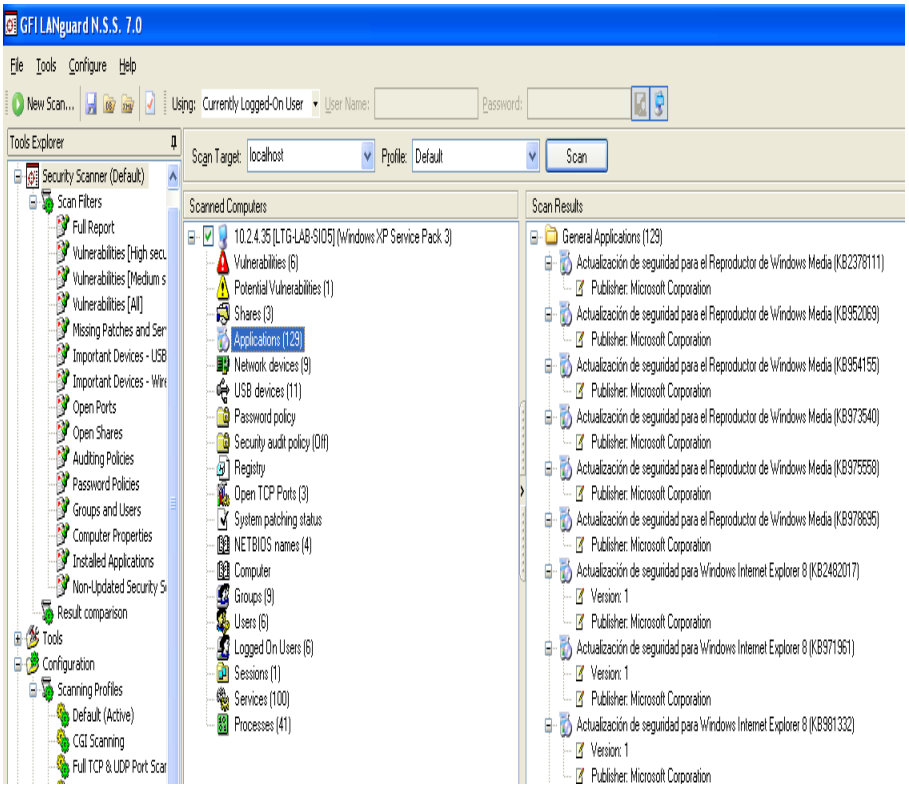


Figura 4.10 Nodo Aplicaciones.

6. Network devices:

Hacer clic en el sub-nodo Network Devices para acceder a la lista de dispositivos y componentes de red (por ejemplo, tarjetas de red cableadas e inalámbricas) que están instaladas en un ordenador objetivo analizado. Utilice esta información para analizar e identificar dispositivos no autorizados conectados en su red. (Ver Figura 4.11)

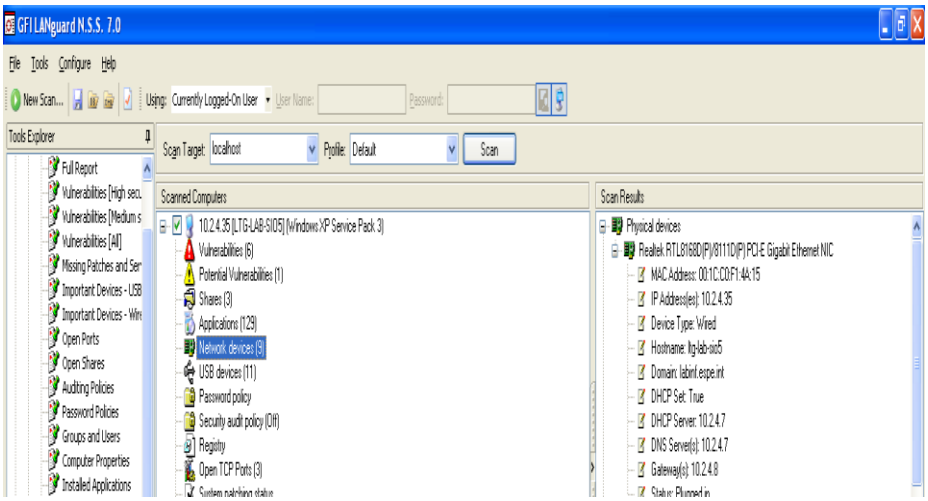


Figura 4.11 Nodo de Network devices

7. USB devices.

Hacer clic en el sub-nodo USB Devices para acceder a la lista de dispositivos USB conectados al ordenador(es) La información recogida en este sub-nodo para identificar dispositivos USB no autorizados conectados actualmente al ordenador. Estos dispositivos no autorizados pueden incluir dispositivos de almacenamiento portátil tales como el Apple iPod, o Creative Zen así como también dispositivos inalámbricos USB y llaves Bluetooth. (Ver Figura 4.12)

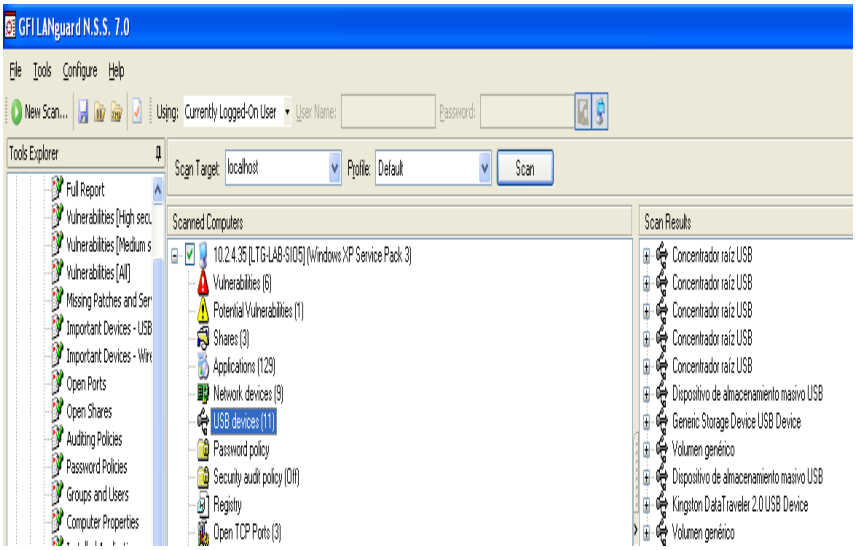


Figura 4.12 Nodo de USB devices

8. Password policy:

Hacer clic en el sub-nodo Password Policy para ver los ajustes de la directiva de contraseñas del ordenador analizado. Estas son esenciales para la aplicación de una red segura. Las vulnerabilidades típicas en una infraestructura de contraseñas débiles las cuales se hacen con pocos caracteres por ejemplo, contraseñas en blanco o por defecto, o contraseñas iguales al nombre de usuario. (Ver Figura 4.13)

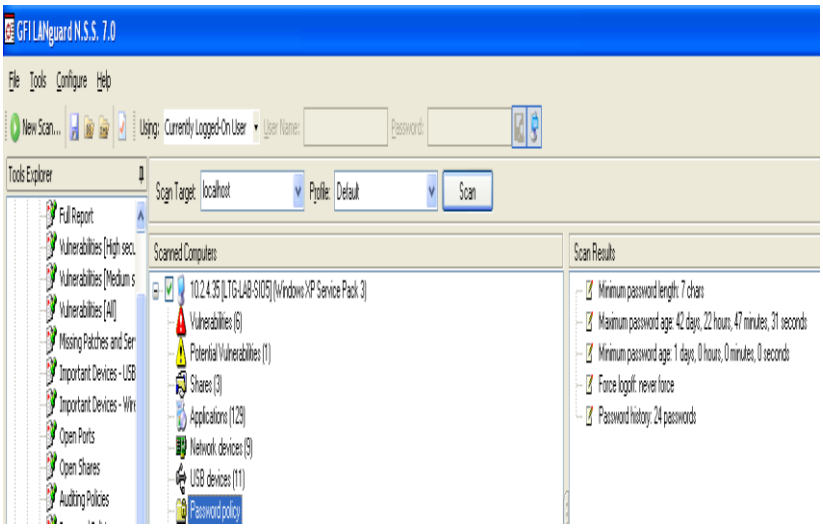


Figura 4.13 Nodo de Password policy

9. Registry:

Hacer clic en el sub-nodo Registry para ver los valores de importantes claves del registro configurado en el ordenador. Esta información permite identificar, aplicaciones autorizadas o no autorizadas así como también aplicaciones válidas que pueden proveer acceso remoto a su red. (Ver Figura 4.14)

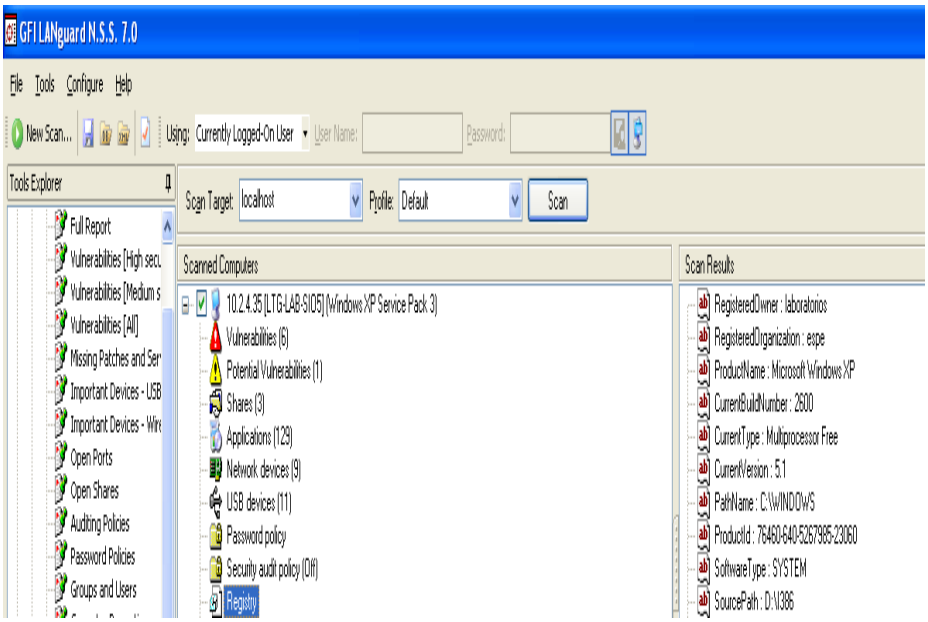


Figura 4.14 Nodo Registry.

10. Open TCP Ports:

Hacer clic en el sub-nodo Open Ports para ver una lista de puertos que son detectados como abiertos en un ordenador analizado. Los puertos abiertos representan servicios activos y aplicaciones que pueden ser explotados por usuarios malintencionados para obtener acceso al ordenador. Es muy importante dejar sólo los puertos que el administrador sabe que son necesarios para las funciones centrales y básicas de red. (Ver Figura 4.15)

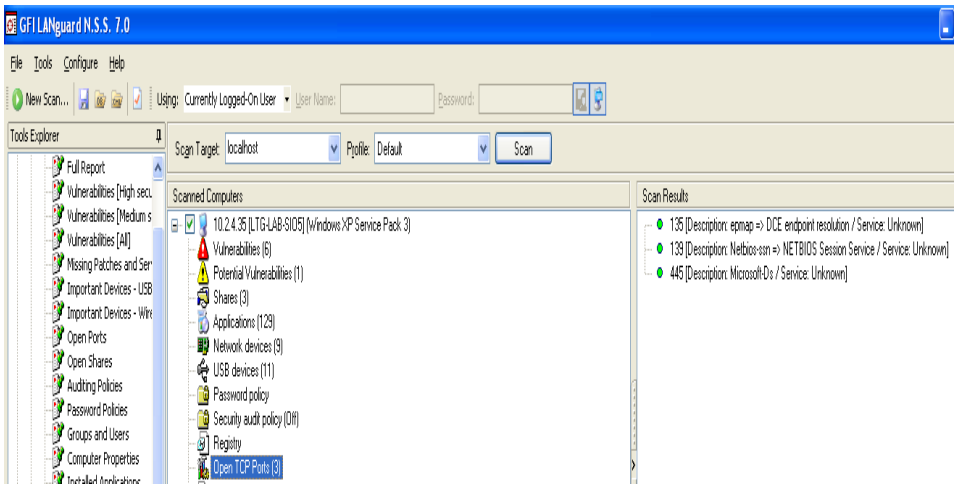


Figura 4.15 Nodo Open TCP ports

11. Netbios

Hacer clic en el sub-nodo NETBIOS names para acceder a la lista de nombres enumerados durante un análisis de un ordenador. Cada ordenador en una red tiene un único nombre NetBIOS. El nombre NetBIOS es una dirección de 16 bytes que permite identificar los recursos en la red. (Ver Figura 4.16)

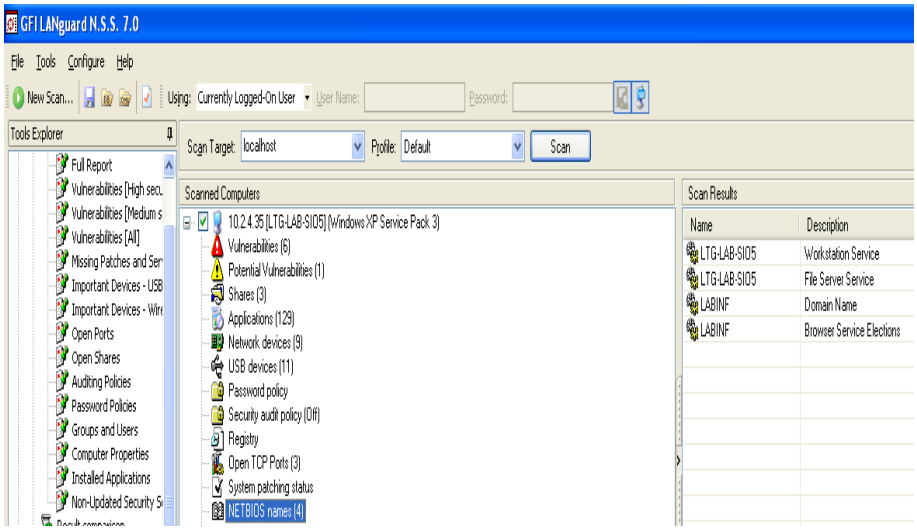


Figura 4.16 Nodo NetBIOS.

12. Computer:

Hacer clic en el sub-nodo Computer para acceder a detalles particulares sobre el ordenador analizado. Los detalles enumerados en este nodo incluyen: (ver Figura 4.17)

- MAC: Muestra la dirección MAC de la tarjeta de red que el ordenador objetivo está usando para conectarse a la red.
- Time To Live (TTL): Muestra el máximo número de saltos de red permitidos antes que un paquete de datos expire.
- Network Role: Denota si el ordenador objetivo analizado es una estación de trabajo o un Servidor.
- Domain: Indica los detalles del dominio o grupo de trabajo. Cuando se analizan objetivos que son parte de un dominio, este campo muestra la lista de dominios de confianza. Si el ordenador objetivo

analizado no es parte de un dominio, este campo mostrará el nombre del respectivo Grupo de Trabajo.

- LAN Manager: Muestra el tipo de sistema operativo y LAN Manager en uso (por ejemplo, Windows 2000 LAN Manager).
- Language: Muestra el idioma configurado en el ordenador objetivo analizado (por ejemplo, Inglés).

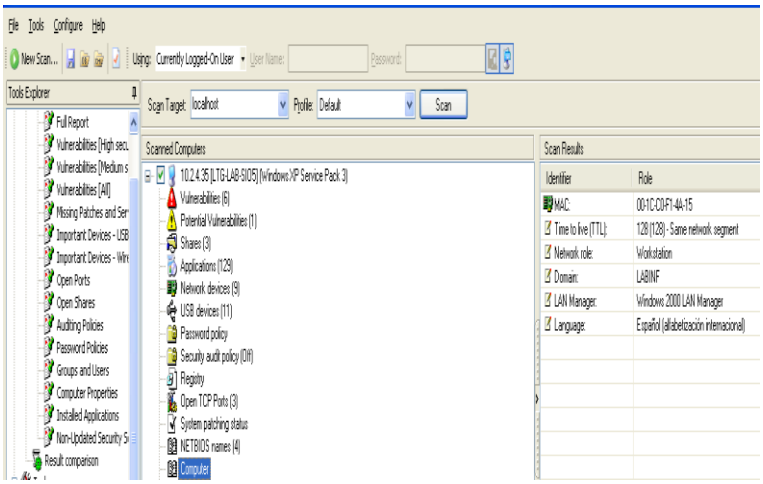


Figura 4.17 Nodo Computer

13. Grupos:

Hacer clic en el sub-nodo Groups para ver todos los grupos locales en el ordenador analizado. (Ver Figura 4.18)

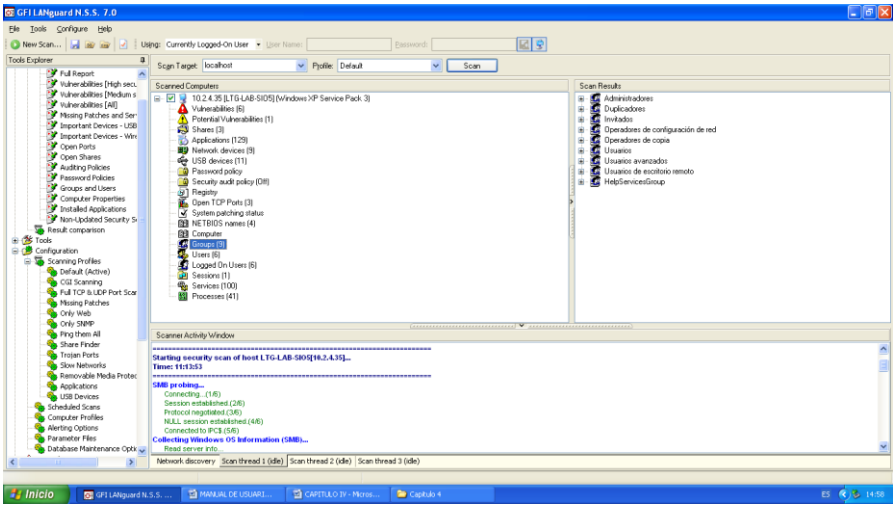


Figura 4.18 Nodo groups.

14. Users:

Hacer clic en el sub-nodo Users para ver todas las cuentas de usuario locales en el ordenador. Esta información para identificar usuarios que pueden permitir el acceso a visitantes "Invitado". (Ver Figura 4.19)

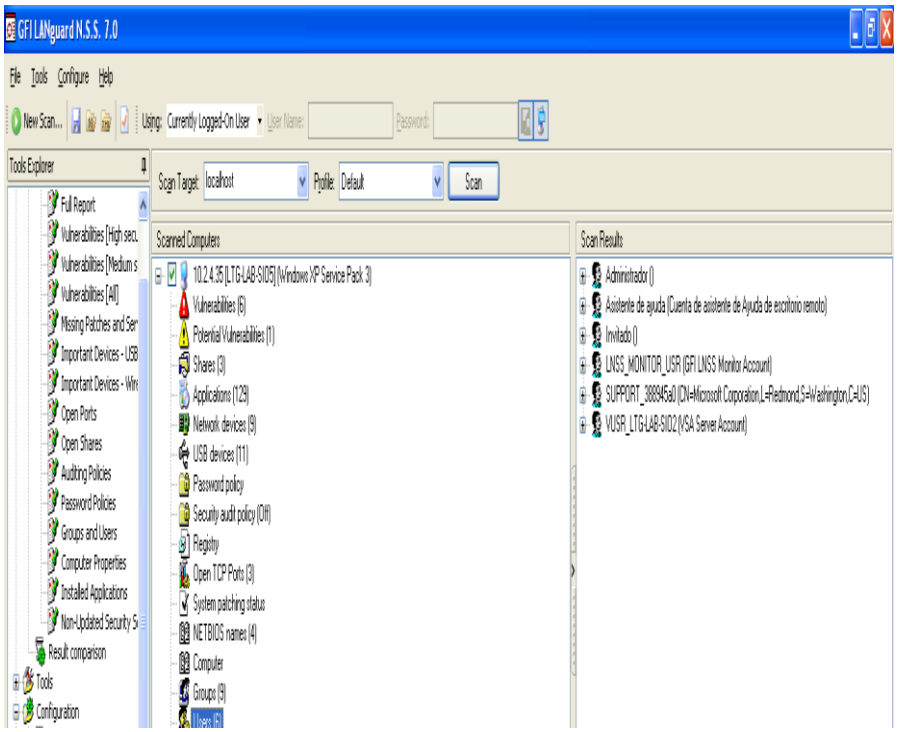


Figura 4.19 Nodo Users.

15. Logged On Users:

Hacer clic en el sub-nodo Logged on Users para acceder a la lista de usuarios que están logados localmente (vía inicio de sesión interactivo) o remotamente en el ordenador analizado. (Ver Figura 4.20)

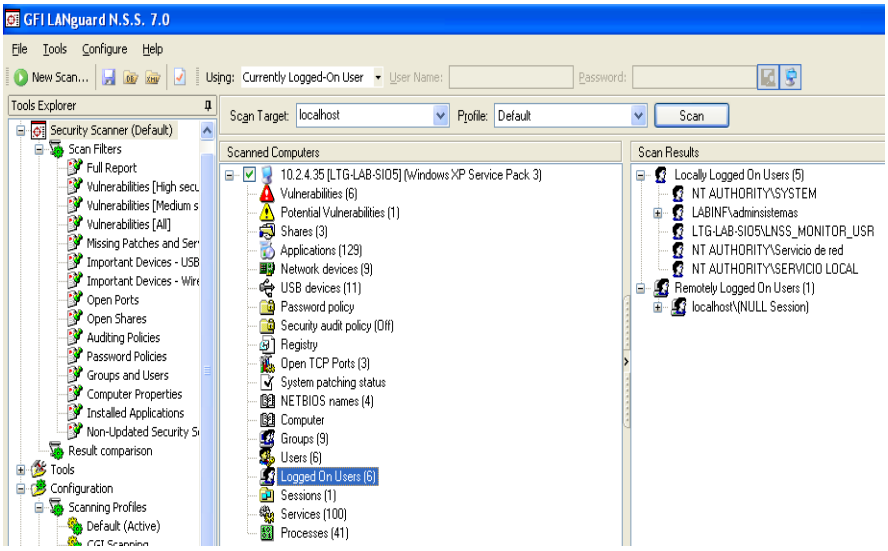


Figura 4.20 Nodo logged On Users.

16. Sessions:

Hacer clic en el sub-nodo Sessions para acceder a la lista de sistemas que están conectados remotamente al ordenador durante el análisis. (Ver Figura 4.21)

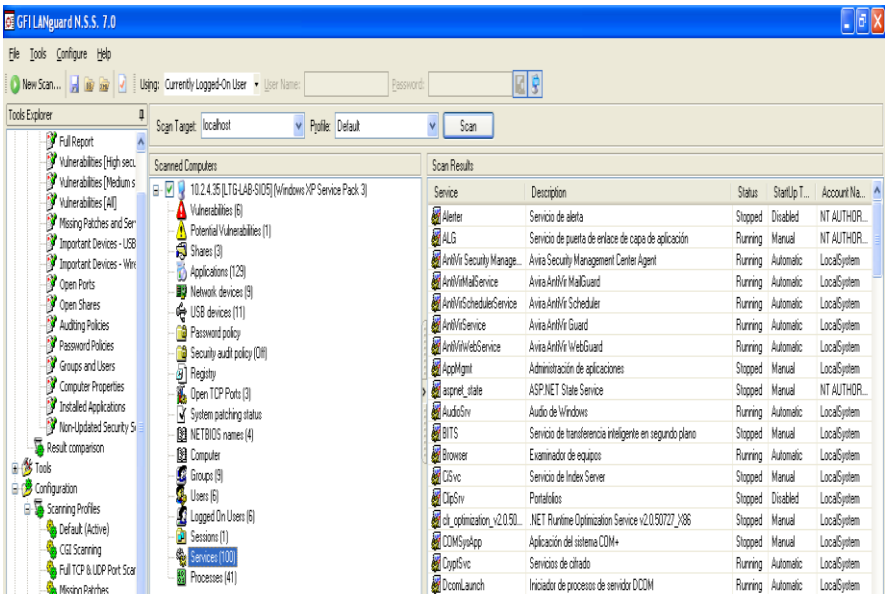


Figura 4.21 Nodo Sessions.

17. Services:

Hacer clic en el sub-nodo Services para acceder a la lista de servicios de alerta. (Ver Figura 4.22)

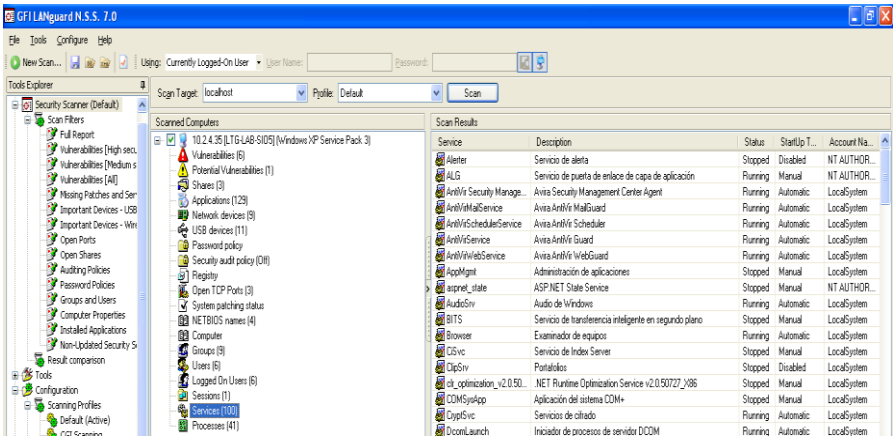


Figura 4.22 Nodo services

18. Proceses:

Hacer clic en el sub-nodo Proceses para acceder a la lista de procesos que se están ejecutando. (Ver Figura 4.23)

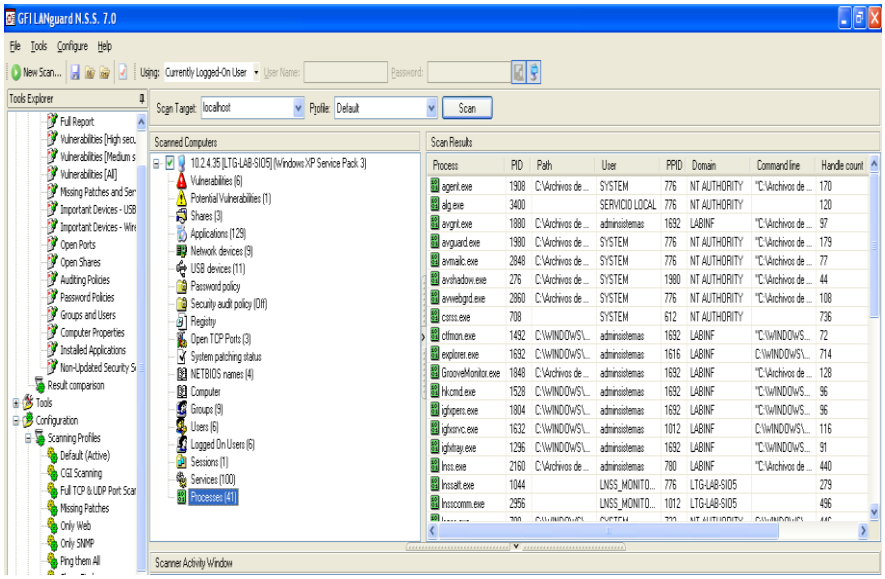


Figura 4.23 Nodo proceses

4.2 PRESENTACION DE RESULTADOS.

Una vez recogida y procesada la información, es necesario presentar los resultados de manera adecuada de tal forma que contribuya una mejor compresión de los objetivos existentes en el manual. En donde podemos detallar los siguientes parámetros:

- Qué se ha pretendido hacer en este proyecto.
- Por qué razón es importante el tema.
- Cuál es la hipótesis del trabajo.
- Cómo se ha llevado a cabo la investigación.
- Cuál es el resultado obtenido.

a. Qué se ha pretendido hacer en este proyecto.

Hacer un documento lo que es estrictamente necesario mantener una secuencia lógica, citando todas y cada una de las expectativas del software utilizado en este trabajo.

b. Por qué razón es importante el tema.

El objetivo es contribuir al desarrollo y control de las redes informáticos utilizando un software que permita capturar toda la información y datos de varios computadores conectados hacia la red, En determinados períodos causando pérdida de tiempo que emplean los administradores en los laboratorios verificando cada PCs, por lo cual es necesario instalar Languard Network Security en un servidor que controle toda la Red.

c. Cuál es la hipótesis del trabajo.

Responde a las inferencias o creencias del investigador, es decir aquella que utiliza para dar una explicación al fenómeno investigado, ya que muestra cuantitativamente la determinación del problema planteado. De este modo tratar de explicar la importancia del software GFI LANguard Network Security que permite crear fácilmente evaluaciones de vulnerabilidad a través de una sencilla pantalla de configuración asistida.

d. Cómo se ha llevado a cabo la investigación.

La investigación fue un proceso que, mediante la aplicación de métodos científicos, procura a obtener información relevante, e imparcial para extender, verificar, corregir o aplicar conocimientos. De los trabajos que responden a los diferentes necesidades planteadas por un problema en una situación determinada de solución.

- **Los objetivos de la investigación.-** Por lo general, se realizó un estudio para describir el monitoreo y escaneo de la red de los Laboratorios Informáticos para dar respuestas satisfactorias, a fin de obtener datos suficientes que permitan hacer ciertas proyecciones directas, que nos da la oportunidad de participar activamente en trabajos creativos de la Comunidad Politécnica.

- **Fuente de la investigación.-** En este proceso se ha utilizado varias formas de obtener información como son: Internet, monografías, tesis, manuales y la información del personal técnico administrativo; esta es la parte que indica exactamente la importancia para desarrollar del trabajo.

e. Cuál es el resultado obtenido.

En este proceso se detalla sobre el monitoreo y escaneo realizado, que serán de gran ayuda para el usuario, ya que constituyen una forma sintetizada y más comprensible de mostrar el manejo de cada una de la herramientas que conforma el software (LANguard Network Security Scanner).

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

El objetivo fundamental de este trabajo es elaborar la documentación de la red LAN de los laboratorios de Redes Informáticos. Utilizando el Software (Languard Network Security Scanner). A fin de facilitar la organización y control interno en esta área. Una vez concluido el proceso de la investigación se pudo observar la gran importancia de tener instalado el software empleando una arquitectura cliente/servidor con todo los privilegios del administrador, a continuación se presentan las siguientes conclusiones.

- La documentación de la Red LAN es parte esencial constituyéndose un documento para el óptimo funcionamiento de la misma, tanto así que la carencia de esta hace que sea un problema fundamental para los técnicos encargados al momento de identificar a los equipos que han sufrido algún cambio tanto por software como hardware.
- La documentación ayudará a aclarar las ideas y brindar las respuestas, para que cada uno de los técnicos encargados en la administración de la Red LAN de los laboratorios Informáticos encuentre sus propias soluciones para los diversos problemas que podrán darse a la hora de cambios o implementación de otros laboratorios en cualquier momento.
- Los recursos (fuentes de consulta) recogidos en esta documentación, son información del personal encargado de la administración de la red de los laboratorios, y que por tanto en cualquier momento pueden desaparecer o cambiar de dirección. Para evitar este riesgo, se ha realizado la documentación de cada uno de ellos.

- El emplear software que escanee la red nos permitió de gran manera recopilar la documentación para el presente trabajo y mantener un historial de funcionamiento y operatividad de la red.
- El software permite identificar puertos abiertos, datos compartidos, detalle relativo a la seguridad y fallas que se producen por la mala utilización de los equipo por parte de los usuarios (alumnos).

- Programas como: Network Inspector, Ethereal, Netstumblers, Languard Netword Security Scanner son empleados para el monitoreo y escaneo de la red, pero se ha elegido utilizar Languard Netword Security debido a que sus módulos recopilan la información (configuración) de los dispositivos instalados en una red de datos.(Ejemplo swichs, routers ect)

5.2. RECOMENDACIONES

- Es importante disponer de un software actualizado para el monitoreo y escaneo constante de la Red, lo que permitirá verificar la eficiencia del sistema.
- Establecer seguridad a nivel de la red para evitar intrusos.
- Actualizar la documentación en diferentes períodos.
- Realizar el monitoreo de la red con frecuencia.
- Hacer una retroalimentación de ciertas políticas realizadas para la administración.
- Tener información sobre el software para distribuir a los diferentes laboratorios que deseen utilizar un escaneo de los dispositivos de red.

BIBLIOGRAFIA

D.K. SATTAROV. Fibra Óptica Tomo 1. Ed. Vocento. España. Pág. 185 – 192.

LINKOGRAFÍA

http://html.rincondelvago.com/redes-lan_1.html

http://www.frm.utn.edu.ar/comunicaciones/redes.html

http://www.google.com.ec/images?hl=es&source=imghp&biw=1167&bih=465&

q=redes&gbv=2&aq=f&aqi=g10&aql=&oq=&gs_rfai=

http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local

http://es.kioskea.net/contents/technologies/ethernet.php3

http://www.monografias.com/trabajos30/redes-de-datos/redes-de-datos.shtml

http://www.mastermagazine.info/termino/4920.php

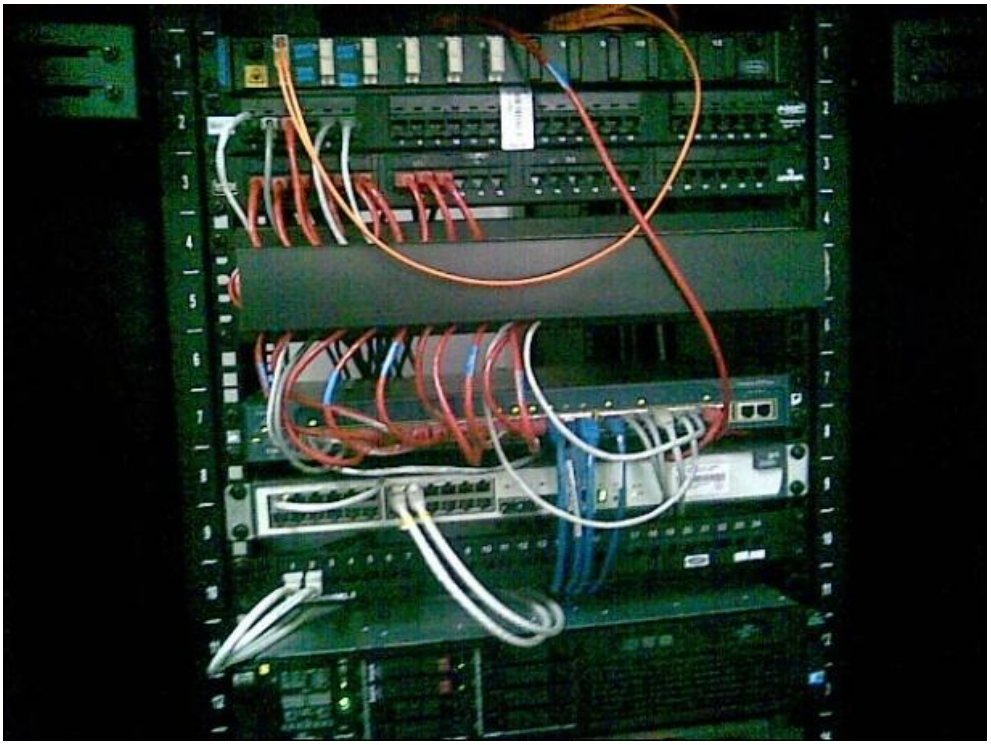
http://www.ordenadores-y-portatiles.com/wimax.html

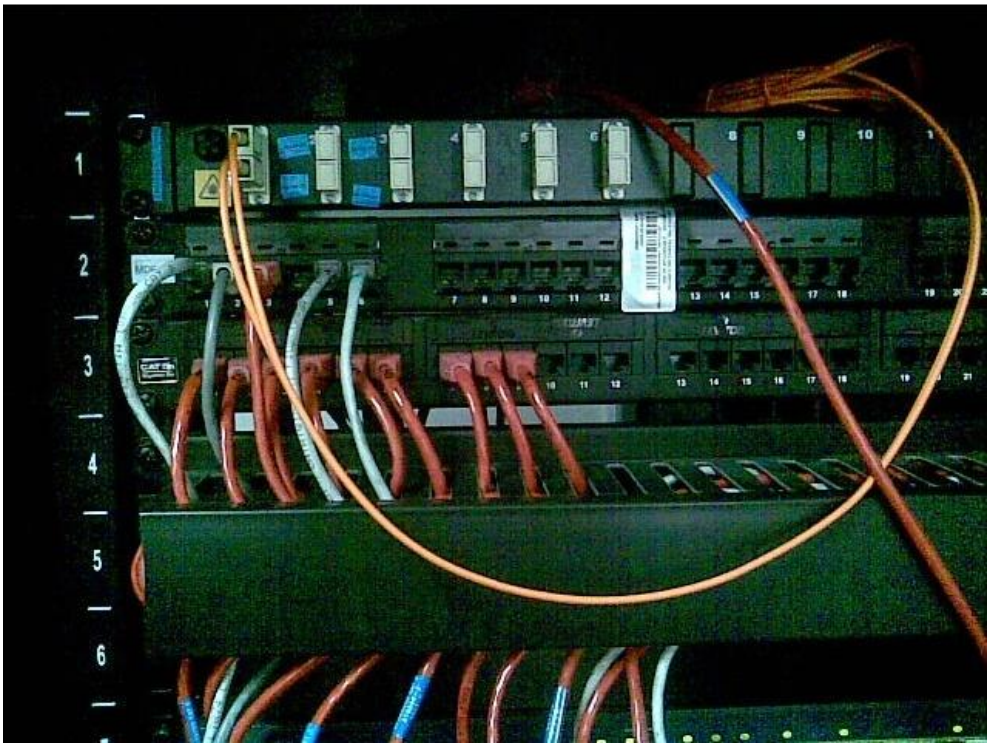
http://www.misrespuestas.com/que-es-wifi.html

http://www.fediea.org/legisla/o241188.php

http://html.rincondelvago.com/ethernet_1.html

ANEXOS





CERTIFICACIÓN

Se certifica que el presente trabajo fue desarrollado por Luis Rolando Ninasunta Guanoquiza y Segundo Manuel Anguisaca Travez, bajo nuestra supervisión.

APROBADO POR:

_____

Ing. César Naranjo

DIRECTOR DEL PROYECTO

_____

Ing. Mayra Salazar

CODIRECTOR DEL PROYECTO

_____

Ing. José Luis Carrillo

CORDINADOR DE LA CARRERA DE SISTEMAS E INFORMÁTICA

_____

Dr. Rodrigo Vaca

SECRETARIO ACADÉMICO ESPE-L