TRABAJO ESPECIAL DE GRADO

# DISEÑO DE LA RED METROPOLITANA Y LA RED LOCAL EN NODO CENTRAL PARA LA COMPAÑÍA SUPRA CARACAS

Presentado ante la Ilustre
Universidad Central de Venezuela
por el Br. Bazán O. Omar Alberto
para optar al Título de Ingeniero
Electricista.

Caracas, 2012

TRABAJO ESPECIAL DE GRADO

# DISEÑO DE LA RED METROPOLITANA Y LA RED LOCAL EN NODO CENTRAL PARA LA COMPAÑÍA SUPRA CARACAS

PROFESOR GUÍA: Prof. Lorena Nuñez
TUTOR INDUSTRIAL: Ing. Ricardo Santana

Presentado ante la Ilustre
Universidad Central de Venezuela
por el Br. Bazán O. Omar Alberto
para optar al Título de Ingeniero
Electricista.

Caracas, 2012

# CONSTANCIA DE APROBACIÓN

Caracas, 09 de noviembre de 2012

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por el Bachiller Omar A. Bazan O., titulado:

**"DISEÑO DE LA RED METROPOLITANA Y LA RED LOCAL EN EL NODO CENTRAL PARA LA COMPAÑÍA SUPRA CARACAS"**

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Comunicaciones, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.

Prof. William Jota
Jurado

Prof. Carlos Moreno
Jurado

Prof. Lorena Núñez
Prof. Guía

# DEDICATORIA

Quiero dedicarle este trabajo a la vida, por ser tan perfecta en su funcionamiento, siempre enseñándonos que somos nosotros mismos el motor de nuestra creación.

A mi padre por haber sido el brazo firme donde apoyarme y a mi madre por ser siempre el soporte perfecto, los amo. Gracias por todo lo que me han dado.

# AGRADECIMIENTOS

A la más grandiosa casa de estudio la Universidad Central de Venezuela, por haberme formado como profesional y como persona.

A los profesores que me acompañaron a lo largo de mi carrera.

A mis tutores, Lorena Nuñez y Ricardo Santana por ser tan especialmente atentos y dedicados en su labor de educar y orientar.

Un especial agradecimiento a mi hermosa novia y amiga Andrea Hernández Motamayor, por ser tan única con su ayuda y aliento. Sin ti el sueño no se hubiese materializado tan armónicamente, te amo. ¡Muchas Gracias!

A María Auxiliadora Rojas por ser tan hermoso ejemplo de dedicación y nobleza, ¡gracias María!

A mis compañeros de trabajo de Supra-Caracas por su ayuda y apoyo.

A mis amigos por creer sólidamente en mí, alentarme y apoyarme. ¡Gracias hermanos, lograremos todo!

**Bazán O., Omar A.**

**DISEÑO DE LA RED METROPOLITANA Y LA RED LOCAL EN NODO CENTRAL PARA LA COMPAÑÍA SUPRA CARACAS**

**Profesor Guía: Lorena Nuñez. Tutor Industrial: Ing. Ricardo Santana. Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Comunicaciones. Institución: Supra-Caracas. Trabajo de grado. 2012. 108 h + anexos**

**Palabras Claves;** Redes WAN, LAN, interconexión, comunicación, automatización de procesos.

**Resumen.** Con la finalidad de solventar el problema de comunicación entre las sedes de la Compañía Supra-Caracas y proporcionar servicios que faciliten y optimicen los procesos que se desarrollan en esta empresa, se plantea el diseño de una red WAN que interconecte las sedes que conforman la institución. Para esto se realizó un levantamiento de información en las cuatro sedes que conforman Supra-Caracas: las Mayas, Artigas, Zona Rental y la Yaguara. Se seleccionó como nodo central para el diseño de la red local (LAN), la sede ubicada en las Mayas, siendo ésta la que posee mayor cantidad de usuarios y donde se realiza el grueso de las actividades operativas y administrativas. Se establecieron las topologías físicas y lógicas para las redes WAN y LAN de acuerdo a las necesidades observadas en el levantamiento de información. Así mismo, se dimensionó el ancho de banda para los enlaces y se realizó una propuesta de los equipos necesarios para la implementación del diseño, además de los parámetros a tomar en cuenta al momento de configurar dichos dispositivos. Con la implementación de este diseño la empresa aumentará significativamente su rendimiento, sus sedes intercambiarán información relevante de forma rápida y eficiente, haciendo posible la automatización de procesos como: pago de nómina, control de asistencia, recaudación de impuestos, entre otros. Además será posible la implementación de servicios como: VoIP, Video IP, asistencia remota y correo electrónico, sobre una plataforma propia de la compañía aumentando los canales de comunicación para la coordinación de las actividades y disminuyendo costos al no contratar estos servicios a otras empresas.

# INDICE GENERAL

**CONSTANCIA DE APROBACIÓN** ..... iii

**DEDICATORIA** ..... iv

**AGRADECIMIENTOS** ..... v

**RESUMEN** ..... vi

**INDICE GENERAL** ..... vii

**LISTA DE FIGURAS** ..... x

**LISTA DE TABLAS** ..... xi

**ACRÓNIMOS** ..... xii

**INTRODUCCIÓN** ..... 1

**CAPÍTULO I** ..... 2

**1 DEFINICIÓN DEL PROBLEMA** ..... 2

1.1 Institución donde se realizó el trabajo de grado ..... 2

1.2 Planteamiento del problema ..... 5

1.3 Objetivos del proyecto ..... 6

Objetivo general ..... 6

Objetivos Específicos ..... 6

1.4 Justificación del proyecto ..... 7

**CAPITULO II** ..... 9

**2 MARCO TEÓRICO** ..... 9

2.1 Antecedentes de la Investigación ..... 9

2.1.1 El modelo OSI ..... 10

2.1.2 Aproximación al modelo de arquitectura de los protocolos TCP/IP ..... 12

2.1.3 Redes Cliente / Servidor ..... 13
2.1.4 Red de área local (LAN) ..... 15
2.1.5 Red de área metropolitana (MAN) ..... 15
2.1.6 Red de área amplia (WAN) ..... 15
2.1.1 Internet ..... 16
2.1.2 Topologías ..... 16
2.1.3 Aplicaciones y Servicios ..... 22
2.1.4 Protocolos de Transporte ..... 27
2.1.5 Protocolos de red ..... 28
2.1.6 Acceso a La Red ..... 44
**CAPITULO III** ..... 59
**3 LEVANTAMIENTO DE INFORMACIÓN** ..... 59
3.1 Evaluación de las necesidades ..... 59
3.1.1 Artigas ..... 59
3.1.2 La Yaguara ..... 60
3.1.3 Zona Rental ..... 61
3.1.4 Las Mayas (Nodo central) ..... 62
3.1.5 Totalización de datos ..... 66
**CAPITULO IV** ..... 68
**4 DISEÑO Y PROPUESTA DE LAS REDES** ..... 68
4.1 Red WAN ..... 68
4.1.1 Topología lógica ..... 68
4.1.2 Topología física ..... 73
4.2 Propuestas para redes de área local (LAN) de las sedes ..... 74

4.3 Dimensionamiento de ancho de banda ..... 84
**CAPITULO V** ..... 88
**5 EQUIPOS Y CONFIGURACIONES** ..... 88
5.1 Selección de equipos y proveedores de servicio ..... 88
5.1.1 Proveedores de servicios ..... 88
5.1.2 Equipos ..... 89
5.2 Propuesta de configuración de equipos ..... 91
5.2.1 Configuración de VLAN ..... 92
5.2.2 Lista de acceso (ACL) ..... 93
5.2.3 Creación de subredes (Subneteo) ..... 94
5.2.4 Enrutamiento ..... 96
5.3 Solución CANTV ..... 97
**CONCLUSIONES** ..... 100
**RECOMENDACIONES** ..... 102
**REFERENCIAS BIBLIOGRAFICAS** ..... 105
**BIBLIOGRAFÍA** ..... 108

# LISTA DE FIGURAS

Figura 2-1.Capas modelo OSI ..... 11
Figura 2-2. OSI vs TCP/IP ..... 12
Figura 2-3. Diagrama de envío y recepción de datos (TCP/IP) ..... 13
Figura 2-4. Red cliente servidor ..... 14
Figura 2-5. Ejemplo de una red WAN ..... 16
Figura 2-6. Topología bus ..... 17
Figura 2-7. Topología de anillo ..... 18
Figura 2-8. Topología estrella ..... 19
Figura 2-9. Backbone serial ..... 21
Figura 2-10 . Backbone distribuido ..... 22
Figura 2-11. Diagrama VPN ..... 48
Figura 2-12. Caminos de datos seleccionado por STP ..... 50
Figura 2-13. Ejemplo de VLANS ..... 50
Figura 2-14. Red 10Base-T ..... 52
Figura 2-15. Red 100Base-T ..... 53
Figura 2-16. TIA/EIA 568A ..... 57
Figura 2-17. TIA/EIA 568B ..... 57
Figura 2-18. Fibra multimodo ..... 58
Figura 3-1. Red física original ..... 64
Figura 3-2. Distribución física de los edificios en las Mayas ..... 66
Figura 4-1. Red WAN con topología estrella ..... 69
Figura 4-2. Topología lógica WAN ..... 72
Figura 4-3. Topología física WAN ..... 73
Figura 4-4. Topología lógica de la LAN ..... 79
Figura 4-5. Red jerárquica ..... 80
Figura 4-6. Topología física LAN ..... 82
Figura 5-1. Topologías CANTV ..... 98

# LISTA DE TABLAS

Tabla 2-1. Direcciones IPv4 con Clase ..... 30
Tabla 2-2. Mascaras de Subred ..... 33
Tabla 2-3. Ejemplo cálculo dirección de red ..... 33
Tabla 2-4. Subneteo direcciones clase B ..... 35
Tabla 2-5. Estándares Ethernet ..... 55
Tabla 3-1. Totalización de datos ..... 67
Tabla 4-1. Velocidad de descarga de internet ..... 86
Tabla 4-2. Ancho de Banda para Enlaces entre las sedes y el nodo central ..... 86
Tabla 5-1. Totalización de equipos ..... 91
Tabla 5-2 Acceso VLANS ..... 93
Tabla 5-3. Red Las Mayas (Nodo Central) IP: 192.168.10.0/24 ..... 94
Tabla 5-4. Red Artigas IP: 192.168.11.0/24 ..... 95
Tabla 5-5. Red Yaguara IP: 192.168.12.0/24 ..... 95
Tabla 5-6. Red Zona Rental IP: 192.168.13.0/24 ..... 95

# ACRÓNIMOS

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

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

**IP:** Internet Protocol **(Protocolo de internet)**

**SUPRA:** Servicio Urbano de Procesamiento, Recolección y Aseo

**LAN**: Local Área Network **(Red de Área Local)**

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

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

**UTP:** Unshielded Twisted Pair **(Par trenzado sin Protección)**

**VLL:** Virtual Leased Line **(Línea Virtual Alquilada)**

**VPL:** Virtual Private LAN **(LAN Virtual Privada)**

**VPN:** Virtual Private Networks **(Red Virtual Privada)**

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

**ISP:** Internet Service Provider **(Proveedor de Servicio de Internet)**

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

**NIC:** Network Information Center **(Centro de Información sobre la Red)**

**VoIP:** Voice over IP **(Voz sobre IP)**

**PSTN:** Public Switched Telephone Network **(Red Telefónica Pública Conmutada).**

**ADSL:** Asymmetric Digital Subscriber Line **(Línea Digital de Abonado Asimétrica)**

**STP:** Spanning Tree Protocol

**NOS:** Network Operating System **(Sistema Operativo de Red)**

**UDP:** User Datagram Protocol

**PAT:** Port Address Translation **(Traducción de Puerto de Red)**

**NAT:** Network address Traslation **(Traducción de Dirección de Red)**

**DNAT:** Dinamic Network address Translation **(Traducción de Dirección de Red Dinámica)**

**SNAT:** Static Network address Translation **(Traducción de Dirección de Red Estática)**

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

**OSPF:** Open Shortest Path First

**BGP:** Border Gateway Protocol

**TCP / IP:** Transmission Control Protocol / Internet Protocol

**EIGRP:** Enhanced Interior Gateway Routing Protocol

**MPLS:** Multiprotocol Label Switching

**DWDM:** Dense wavelength Division Multiplexing **(Multiplexación por División en Longitudes de Onda Densas)**

**ICANN:** Internet Corporation for Assigned Names and Numbers **(Corporación que asigna las direcciones IP)**

# INTRODUCCIÓN

La Compañía Supra Caracas es una Institución Pública con participaciones del Ministerio del Poder Popular para el Ambiente, Municipio Libertador y Alcaldía de Caracas, que se encarga de la recolección, procesamiento de desechos y limpieza de gran parte de la ciudad de Caracas. Esta institución fue creada en Agosto del 2011, para sustituir en el trabajo del aseo a la corporación de servicios de la Alcaldía de Caracas.

La institución cuenta con personal administrativo y operativo, maquinaria para el desarrollo de las actividades diarias como una flota de camiones que incluyen: compactadoras de basura, camiones de transferencia, y otros medios de transporte y recolección, así como depósitos y talleres mecánicos que poseen inventarios. La empresa está conformada por cuatro sedes distribuidas en las siguientes zonas: Las Mayas, Artigas, La Yaguara y Zona Rental, las cuales se encargan del manejo de la actividad administrativa, operativa y la coordinación de las actividades necesarias para el desarrollo de las labores de aseo, recolección y procesamiento.

Por ser una compañía creada recientemente, no cuenta con una plataforma tecnológica adecuada a sus necesidades. Por ejemplo, buena parte de su comunicación se realiza a través de correos electrónicos públicos y líneas telefónicas personales. Es por esto que la empresa requiere el diseño e implementación de una plataforma tecnológica que provea los medios adecuados para la realización de las tareas administrativas y operativas de manera óptima.

La compañía necesita medios a través de los que pueda comunicarse de manera rápida y efectiva, además de sistemas que controlen los procesos que en la empresa se desarrollan. El objetivo de este trabajo es proponer una red de datos que sirva como fundamento para la implementación de todos estos servicios.

# CAPÍTULO I

## DEFINICIÓN DEL PROBLEMA

### 1.1 Institución donde se realizó el trabajo de grado

En esta sección se expone la estructura organizacional de la empresa donde se realizó el trabajo especial de grado.

**Sistema Urbano de Procesamiento Recolección y Aseo (Supra – caracas)**

Supra-Caracas es una empresa prestadora del servicio de aseo urbano, recolección de residuos sólidos, barrido, limpieza y lavado de áreas públicas del Distrito Capital suministrándole soluciones integrales en materia medioambiental. Fundada en Agosto del año 2011, por disposición del presidente Hugo Rafael Chávez Frías, como una empresa con gran sentido social que contribuye al desarrollo de la ciudad de Caracas.

La Empresa inició sus actividades dotada de unidades con tecnología innovadora en la recolección, transporte de basura y desechos sólidos garantizando un servicio de calidad y la satisfacción de las necesidades de todos los habitantes de Caracas.

**Misión**

Preservar el medio ambiente para mejorar la calidad de vida de los caraqueños, así como mantener la ciudad libre de residuos sólidos, con alta eficiencia

y mejora continua de los procesos, en busca de la identificación de los trabajadores con la empresa para lograr eficazmente los objetivos organizacionales.

**Visión**

Mantenerse como la empresa líder en servicios medioambientales de gran sentido social, enmarcada en los más altos principios de moral, ética profesional, con excelente clima organizacional, para satisfacer las necesidades de los caraqueños, en la recolección y saneamiento de todas las calles de la ciudad capital.

Para conseguir el logro anterior, SUPRA - CARACAS cuenta con un personal altamente calificado, leal, con una visión clara y estratégica, identificado y comprometido con una filosofía de trabajo orientada siempre a la participación activa y social del pueblo en el desarrollo de los proyectos, sin importar la envergadura de los mismos y al logro de todos los objetivos propuestos por la organización.

**Objetivo General**

SUPRA - CARACAS cumple con el objetivo de operar eficazmente como ente clave del negocio de recolección de basura y desechos sólidos, así como también de la limpieza y saneamiento de toda la ciudad, a través de la prestación de servicios eficientes a nuestros habitantes.

**Objetivos Específicos**

1. Desarrollar, mantener, instrumentar, fusionar, simplificar y optimizar los procesos de la organización, con la finalidad de garantizar una alta productividad y un uso adecuado de los recursos humanos, financieros, tecnológicos y materiales de la empresa, para obtener una mayor confiabilidad en los recursos finales.

2. Dedicar tiempo y recursos humanos, para evaluar las necesidades de la ciudadanía y responderlas en materia de procesamiento, recolección y aseo la ciudad de Caracas.

3. Contratar personal de excelente capacidad profesional.

4. Motivar y desarrollar actividades tendentes al bienestar económico, social, cultural y deportivo de los trabajadores.

5. Mantener y crear incentivos para los trabajadores y administrativos, que motiven su permanencia dentro de la organización.

6. Mantener y desarrollar relaciones humanas, profesionales, y honestas para la mejora continua de la calidad del ambiente de trabajo.

7. Cumplir con la normativa legal vigente que regule el funcionamiento idóneo de la empresa.

**Valores**

SUPRA - CARACAS se caracteriza por ser una empresa que posee unos valores organizacionales claramente definidos que garantizan el éxito presente y futuro.

Entre los valores identificados se pueden mencionar:

- ***Continuidad:*** *Proseguir con la misión que se ha iniciado con perseverancia y dedicación.*
- ***Cordialidad:*** *El trato hacia el personal, clientes y proveedores será amistoso, franco y sincero.*
- ***Responsabilidad Social:*** *Cualidad con la cual se responde por los compromisos y actos que se tienen con la ciudadanía caraqueña, proveedores, y trabajadores.*
- ***Honestidad:*** *Calidad, decencia, cumplimiento de los deberes de acuerdo con la moral y las buenas costumbres*

- ***Trabajo seguro:*** *Realizar las labores diarias protegiendo a las personas, equipos, instalaciones y al medio ambiente*

**Estructura Organizacional**

SUPRA - CARACAS, presenta una estructura a nivel organizacional de tipo lineal, es decir que la jerarquía de mando va desde los niveles superiores hasta los inferiores.

Se encuentra encabezada por la Junta Directiva, la cual es la que toma las decisiones más importantes dentro de la organización. Posteriormente encontraremos la Gerencia General, la cual controla las siguientes gerencias: Administración, Recursos Humanos, Operaciones, Tecnología de la Información, Consultoría Jurídica, Recaudación, Ambiental y Educación y por último Seguridad Física y Protección Integral.

## 1.2 Planteamiento del problema

Esta organización cuenta con más de 3500 empleados, con una flota de varias centenas de camiones y varias sedes administrativas y operativas. El no poseer una plataforma de transporte de datos que sirva para comunicar tanto las sedes entre sí, como a los usuarios de cada una de estas, limita la capacidad de respuesta y coarta las posibles mejoras en las actividades diarias de la institución.

Existen requerimientos de servicios específicos para los usuarios en cada una de las sedes, como un servicio de correo electrónico, mensajería instantánea, servicios de voz, navegación, compartición de archivos, impresiones en red, entre otros. Para esto son necesarios servicios y aplicaciones de tipo informático, como servidores de dominio, servidores que manejen DHCP (*protocolo de configuración de host*

*dinámico),* sistema DNS (*servicio de nombre de dominio*), así como servidores que alojan sistemas requeridos por las áreas administrativas (nómina, recaudación de impuestos, etc.) y operativas (inventario, monitoreo de flota, etc.), que deben necesariamente contar con una red de datos para poder funcionar correctamente.

Actualmente no se cuenta con una infraestructura con las características necesarias para proveer estos servicios y ser capaz de garantizar la comunicación entre el personal operativo y los coordinadores, esto trae como consecuencia un retardo notable en todas las actividades que se realizan en la institución.

La inexistencia de una red que haga posible el manejo automatizado de información de la nómina de empleados, administrativa, así como el monitoreo de las unidades móviles, limita notablemente los procesos administrativos haciéndolos más lentos y propensos a fallas e irregularidades.

## 1.3 Objetivos del proyecto

### Objetivo general

Diseñar una red Metropolitana y la red Local en el nodo central para la compañía Supra Caracas, que haga posible la comunicación entre las sedes de manera segura y eficiente, y permita ofrecer los servicios necesarios para coordinar las actividades diarias que se desarrollan en la empresa.

### Objetivos Específicos

- Evaluar las necesidades de cada sede.
- Plantear la topología física y lógica de la red LAN y la red WAN.
- Seleccionar los equipos de comunicaciones y proveedores de servicio necesarios para implementar la topología planteada.

- Dimensionar el ancho de banda para el intercambio de datos entre las sedes.
- Realizar una propuesta de Configuración de los equipos de la red LAN (*en el nodo central*) y la red WAN.

## 1.4 Justificación del proyecto

Debido a la dificultad de comunicación entre las sedes, surge la necesidad de la creación de una red que las interconecte y haga posible el intercambio de información, con el objetivo de que la coordinación de las actividades diarias se desarrolle eficientemente. También es necesaria una red que administre el flujo de datos para así encargarse de la seguridad, dar acceso a navegación y limitar el ancho de banda para cada sede, además de la interconexión entre aplicaciones que permitan monitorear las unidades móviles y conocer la ubicación exacta de las mismas.

Las fallas operativas causan que la basura no pueda ser recolectada en la ciudad, cosa que genera un riesgo de salud pública. La ausencia de una red que no permita el funcionamiento de un sistema que automatice los procesos que implican manipulación de fondos, expone la seguridad de la institución y la hace propensa a fraudes.

Este proyecto tiene como objetivo dar solución a esta problemática mediante el diseño de una red LAN (*Red de área local)* en el nodo central y una red WAN (*Red de área amplia*) para interconectar las distintas sedes entre sí.

La red LAN hará posible la instalación de un centro de datos que alojará los servidores que proveen los servicios y aplicaciones necesarias para las actividades administrativas, y que podrá ser accedido desde cualquiera de las sedes. Adicionalmente, permitirá el acceso a la red de datos por parte de los usuarios, así como las impresiones en línea y otros servicios.

La red WAN permitirá la interconexión entre las redes LAN de cada una de las sedes. De esta manera se garantizará un acceso seguro y controlado a las aplicaciones y servicios que utilizan servidores alojados en el centro de datos, haciendo posible ofrecer servicios como correo electrónico, voz sobre IP e internet, así como la aplicación de políticas de seguridad y la realización de la gestión y administración de toda la red.

Algunas de las aplicaciones que se podrán centralizar, dar acceso desde cada una de las sedes son: sistema de nómina y recursos humanos, de inventario, monitoreo de flota, recaudación de impuestos y la publicación de contenido web.

El nodo central de esta red debe estar constituido por servidores que alojen las aplicaciones y servicios de usuarios, así como herramientas que permitan administrar el acceso a internet, aplicar políticas de seguridad y controlar el flujo de datos de todas las sedes.

# CAPITULO II

# MARCO TEÓRICO

## 2.1 Antecedentes de la Investigación

El manejo de información, gracias a los avances en las tecnologías de comunicaciones, es parte esencial de toda empresa moderna. La automatización de los procesos se apoya fundamentalmente en la capacidad de la empresa para transportar de manera eficiente y oportuna información relevante, ya sea para control de las actividades diarias o para recolección de estadísticas que posteriormente permitan introducir correcciones que mejoren estos procesos. Para esto es necesario que exista una comunicación entre las diferentes sedes, así como entre los diferentes departamentos dentro de una misma localidad.

Las redes de datos son, en conjunto, la solución más eficiente y segura. Además, es una solución práctica debido a que en la ciudad la mayoría de los enlaces físicos necesarios para esta red (*WAN*) ya existen y solo es preciso solicitar el servicio a las empresas de telecomunicaciones que sean propietarias esta infraestructura.

La empresa SUPRA Caracas tiene un claro interés en utilizar herramientas tecnológicas para el mejoramiento de sus actividades en el plano administrativo y operativo. Prueba de esto es la reciente implementación y configuración de un sistema de radios Tetra para la comunicación remota entre el personal, siendo este uno de varios trabajos que adelanta la empresa en este sentido.

## Bases teóricas

En esta sección se conocerán los conceptos y aplicaciones, de las tecnologías necesarias para dar solución al problema planteado, se fundamenta con bases teóricas y normas, extraída de textos y fuentes confiables, los diseños y propuestas expuestos posteriormente en este proyecto.

### 2.1.1 El modelo OSI

Antes de conocer el modelo OSI es importante entender qué es un protocolo. Un protocolo es una serie de reglas que definen los procesos para la realización de una actividad específica. Así, los protocolos pueden definir desde la metodología para construir una empresa hasta los pasos para la fabricación de un tornillo. Los protocolos en redes de computadoras definen las normas para la comunicación entre dispositivos de red. Sin protocolos, los dispositivos no podrían interpretar las señales enviadas por otros dispositivos, y los datos no llegan a ninguna parte. [1]

El Modelo OSI (Open Systems InterConnect) está constituido por 7 capas donde se definen las funciones de los protocolos de comunicaciones. Cada capa del modelo representa una función realizada cuando los datos son transferidos entre aplicaciones a través de una red intermedia.

En las capas no se define un único protocolo sino más bien una función de comunicación que puede ser realizada por varios protocolos. Por ejemplo, un protocolo de transferencia de documentos y otro de correo electrónico, los dos facilitan el servicio de usuario y son parte de la capa de aplicación.

Cada protocolo sólo ha de ocuparse de la comunicación con su igual en la capa equivalente de un sistema remoto, sin preocuparse de la capa superior o inferior.

Sin embargo, también debe haber un acuerdo en cómo pasan los datos de capa en capa dentro de un mismo sistema, pues cada capa está implicada en el envío de datos.

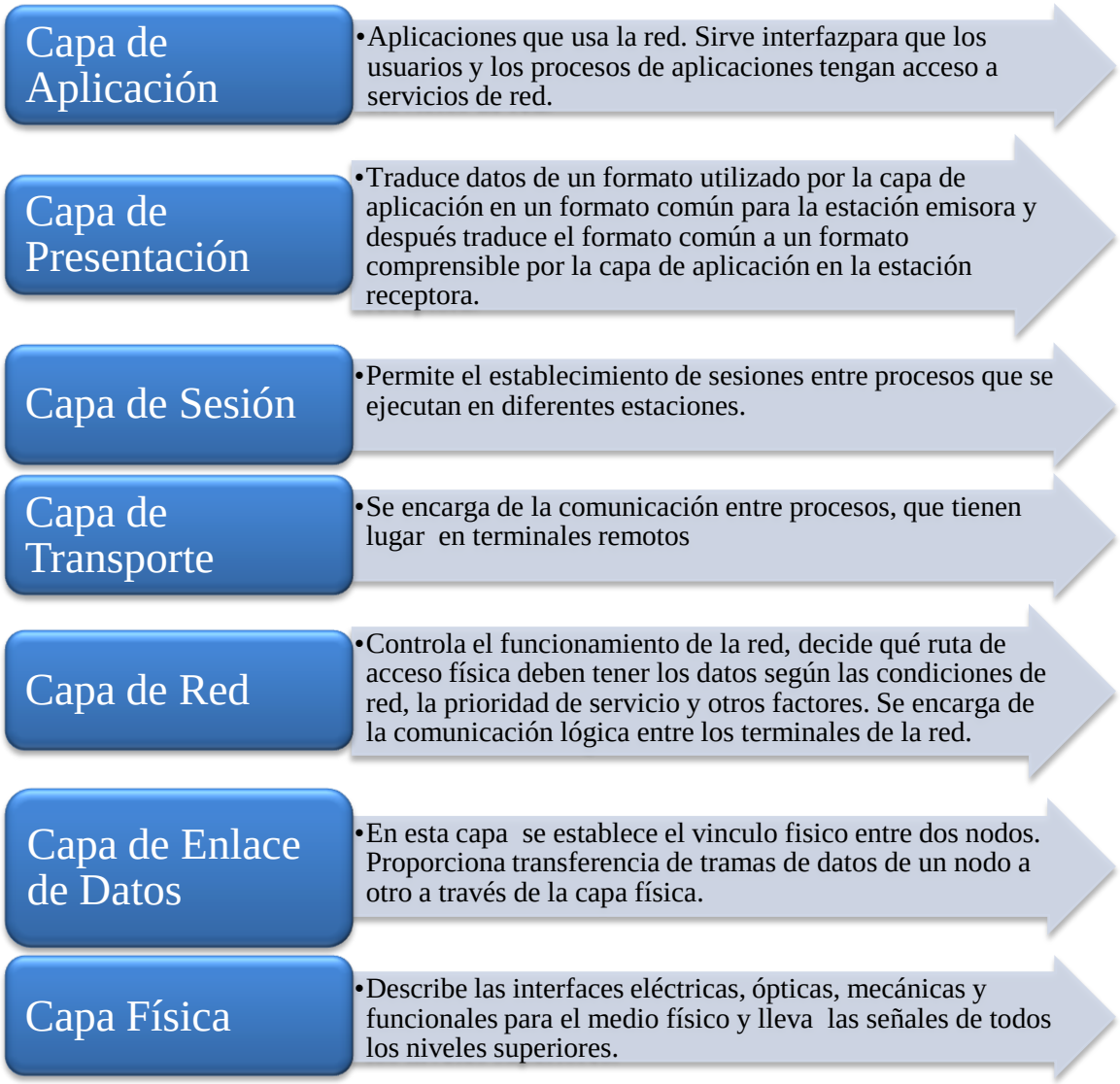


**Figura 2-1.*Capas Modelo OSI***

Las capas superiores delegan en las inferiores la transmisión de los datos a través de la red. Los datos descienden de capa en capa, hasta que son transmitidos a través de la red por los protocolos de la capa física. En el sistema remoto, irán ascendiendo por las capas hasta la de aplicación, una capa da servicio a la capa

superior y requiere servicios de las capas inferiores. En la siguiente figura se muestra de una manera gráfica las capas del modelo OSI.

### 2.1.2 Aproximación al modelo de arquitectura de los protocolos TCP/IP

El modelo de arquitectura de estos protocolos es más simple que el modelo OSI, como resultado de la agrupación de diversas capas en una sola. Así, por ejemplo, la capa de presentación desaparece pues las funciones a definir en ellas se incluyen en las propias aplicaciones.

Lo mismo sucede con la capa de sesión, cuyas funciones son incorporadas a la capa de transporte o de aplicación de los protocolos TCP/IP. Finalmente la capa de enlace de datos no suele usarse en dicho paquete de protocolos, pues sus funciones son realizadas por la capa de acceso a la red. En la siguiente figura se muestra de forma grafica, la comparación del modelo OSI y el modelo TCP/IP.

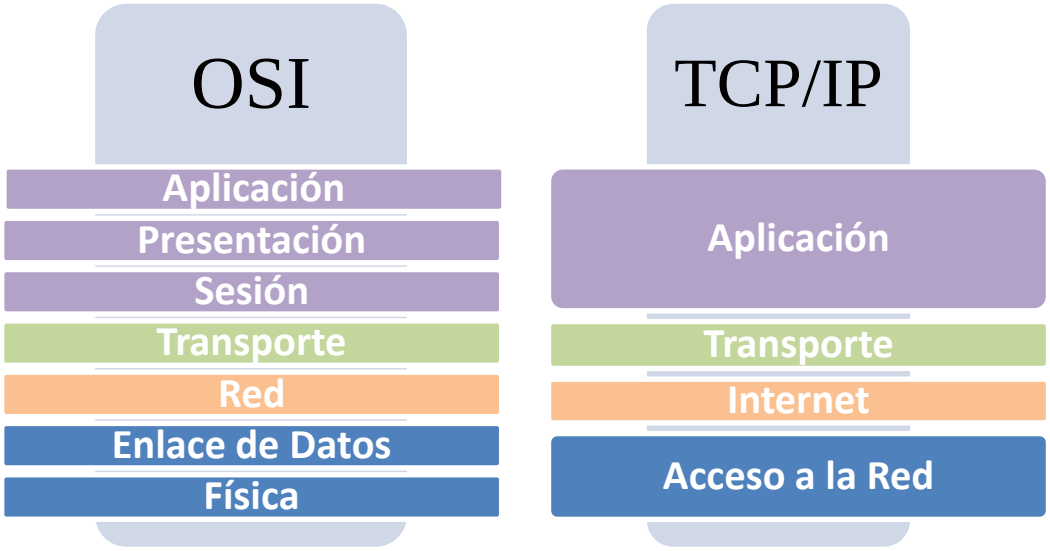


**Figura 2-2.** ***OSI vs TCP/IP***

Al igual que en el modelo OSI, los datos descienden por la pila de protocolos en el sistema emisor y la escalan en el extremo receptor. Cada capa añade a los datos

a enviar a la capa inferior información de control. Esta información de control se denomina **cabecera**, pues se coloca precediendo a los datos. A la adición de esta información en cada capa se le denomina **encapsulación**.

Cuando los datos se reciben tiene lugar el proceso inverso, es decir, según los datos ascienden por la pila, se van eliminando las cabeceras correspondientes.

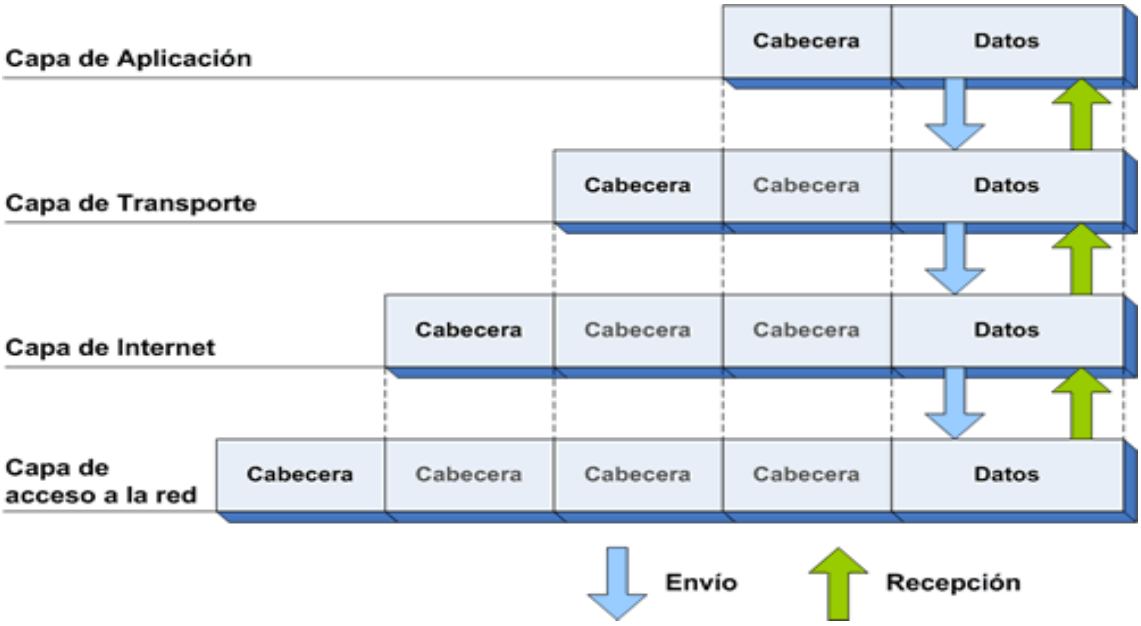


**Figura 2-3.** ***Diagrama de envío y recepción de datos (TCP/IP)***

**Fuente: [2] Textos Científicos, 2006**

### 2.1.3 Redes Cliente / Servidor

Una manera de diseñar una red es usar un ordenador central, conocido como un servidor, para facilitar la comunicación y el intercambio de recursos entre otros equipos de la red, que se conocen como clientes. Los clientes suelen tomar la forma de las computadoras personales, también conocidos como estaciones de trabajo. Este tipo de red utiliza un servidor para dar a cada cliente la configuración básica de manera de garantizar su conectividad. Además, puede permitir a los clientes

compartir y almacenar datos así como ejecutar aplicaciones compartidas. El servidor permite sólo a los usuarios autorizados acceder a sus recursos. [3]

Cada computadora en una red cliente/servidor actúa como un cliente o un servidor. Es posible, pero poco frecuente, que algunos equipos puedan actuar como ambos. La Figura 2-4 ilustra cómo los recursos se comparten en una red cliente/servidor.

Para funcionar como un servidor, un equipo debe ejecutar un sistema operativo especializado para funcionar en red.


**Figura 2-4.** ***Red cliente servidor***

**Fuente: Dean, 2009**

### 2.1.4 Red de área local (LAN)

Como su nombre lo indica, una red LAN es una red de ordenadores y otros dispositivos que se limita a un espacio relativamente pequeño, tal como un edificio o incluso una oficina. A menudo, las redes LAN están interconectadas por separado y se basan en varios servidores que ejecutan diferentes aplicaciones. Esta red puede contener docenas de servidores, cientos de puestos de trabajo, y varios dispositivos de almacenamiento compartido, impresoras, plotters, máquinas de fax, e incluso las interfaces telefónicas. [4]

### 2.1.5 Red de área metropolitana (MAN)

Una red que es más grande que una LAN y conecta a los clientes y servidores de varios edificios, por ejemplo, un grupo de oficinas de gobierno alrededor de un capitolio estatal- se conoce como MAN debido a la distancia que cubre. Una MAN puede usar tecnología de transmisión y medios de comunicación diferente a una red LAN. [5]

### 2.1.6 Red de área amplia (WAN)

Una red que conecta dos o más LANs o MANs geográficamente distantes incluso entre distintos países, se llama WAN. Debido a que tales redes llevan datos a través de distancias más largas que las LAN, las WAN requieren métodos y medios de comunicación ligeramente diferentes de transmisión y a menudo utilizan una mayor variedad de tecnologías que las LAN. La mayoría de las MAN también pueden ser descritas como las WAN, de hecho, es común que los ingenieros se refieran a todas las redes que cubren una zona geográfica amplia como redes WAN. [6]

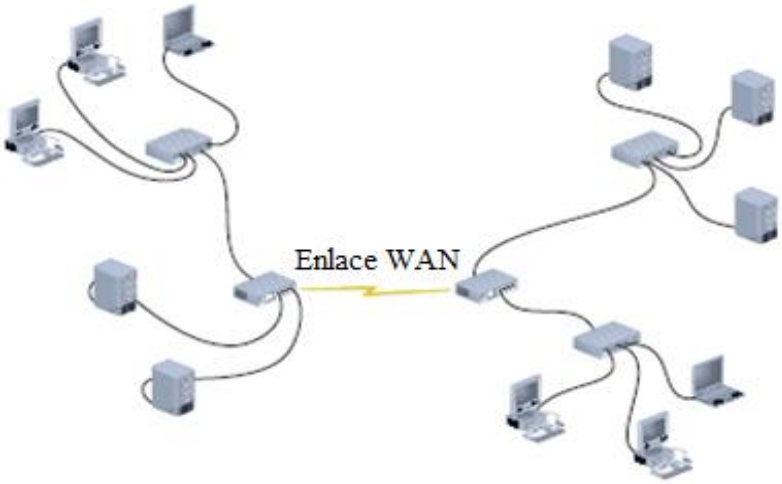


**Figura 2-5.** ***Ejemplo de una red WAN***

**Fuente: Dean, 2009**

### 2.1.1 Internet

Es la red WAN más grande del mundo, este conjunto descentralizado de redes de comunicación interconectadas utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos.

### 2.1.2 Topologías

**Topología física**

Este tipo de topología se refiere a la distribución física o patrón de los nodos de una red, representándola en forma general, es decir, que no especifica los tipos de dispositivos, métodos de conectividad o esquemas de direccionamiento para la red. Las topologías físicas se dividen en tres formas geométricas fundamentales: ***bus, anillo*** *y* ***estrella***. Estas formas se pueden mezclar para crear topologías híbridas.

Antes de diseñar una red, es necesario comprender las topologías físicas, la infraestructura de cableado y los medios de transmisión que se utilizarán. Además esto es necesario para solucionar posibles problemas o cambiar su infraestructura.

- **Topología bus**

Una topología de bus consiste en un cable único, llamado *bus*, que conecta todos los nodos de una red sin la intervención de los dispositivos de conectividad. En la mayoría de los casos el medio físico para esta topología es cable coaxial.

Una topología de bus puede soportar sólo un canal de comunicación. Como resultado, cada nodo comparte la capacidad total del *bus*. Una red de bus es una topología pasiva, en la que cada nodo escucha de forma pasiva para aceptar los datos dirigidos al mismo.

Cuando un nodo desea transmitir datos a otro nodo se emite una alerta a toda la red, informando a todos los terminales que una transmisión está siendo ejecutada; el nodo de destino entonces puede recibir la transmisión sin colisión de paquetes. Los nodos que no sean emisores o receptores ignoran el mensaje. [7]

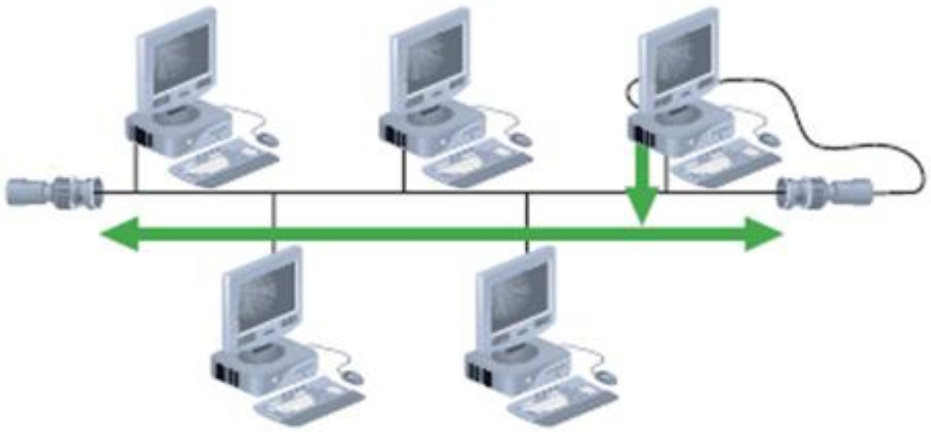

**Figura 2-6.** ***Topología bus***

**Fuente: Dean, 2009**

- **Topología anillo**

En una topología en anillo, cada nodo está conectado a los dos nodos más próximos, de modo que toda la red forma un círculo. En la figura se aprecia como los datos se transmiten hacia la derecha, de forma unidireccional, alrededor del anillo. Cada estación de trabajo acepta y responde los paquetes dirigidos a ella, luego los envía al otro lado de la estación en el anillo.

Cada estación de trabajo actúa como un repetidor para la transmisión. El hecho que todas las estaciones de trabajo participen en la entrega, hace de la topología de anillo una topología activa. La topología de anillo no tiene "extremos" y los datos se detienen en su destino. En la mayoría de redes las de anillo, se utiliza como medio físico par trenzado o cableado de fibra óptica. [8]

**Figura 2-7.** ***Topología de anillo***

**Fuente: Dean, 2009**

- **Topología estrella**

En una topología en estrella, cada nodo de la red está conectado a través de un dispositivo central. Cualquier cable en una red en estrella conecta solamente dos dispositivos (ej: una estación de trabajo y un Switch), por lo que un problema de cableado afectará dos nodos como máximo.

Las topologías en estrella se construyen generalmente con par trenzado o cableado de fibra óptica. Las estaciones de trabajo o impresoras transmiten datos al concentrador (o concentrador), un Enrutador o un Switch, que luego retransmite la señal al segmento de red que contiene el nodo destino. [9]

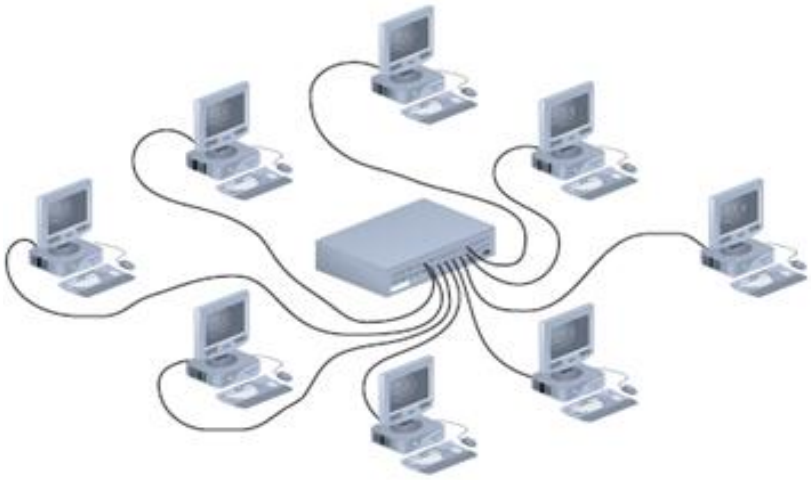

**Figura 2-8.** ***Topología estrella***

**Fuente: Dean, 2009**

## Topologías Lógicas

El término topología lógica, se refiere a la manera en que se transmiten los datos entre los nodos, en lugar de la disposición física de los caminos que toman los

datos. La topología lógica de una red no necesariamente coincidirá con su topología física. Las topologías lógica más comunes son topologías de bus y anillo.

En una topología de bus lógica, las señales viajan desde un dispositivo de red a todos los demás dispositivos de la misma (o segmento de red). Los datos pueden o no, viajar a través de un dispositivo de conexión intermedio (como en una red de topología en estrella). Una red que utiliza una topología de bus física también utiliza una topología de bus lógica. Las redes que utilizan topología física estrella, también dan lugar a una topología de bus lógica.

Por otra parte, en una topología de anillo lógico, las señales han de seguir una trayectoria circular entre emisor y receptor. Las redes que utilizan una topología de anillo puro utilizan una topología de anillo lógico. La topología de anillo lógico también es utilizado por la topología estrella, porque las señales han de seguir un camino circular, incluso a medida que viajan a través de un dispositivo de conexión. [10]

**Backbone de las redes**

La red dorsal del término en inglés *backbone*, es el cableado que conecta los Concentradors, Switches y enrutadores de la red. Por lo general, el medio físico es capaz de presentar un mayor rendimiento que el cableado que conecta estaciones de trabajo a concentradors. Esta capacidad adicional es necesaria porque el backbone transporta más tráfico que cualquier otro cableado de la red.

Por ejemplo, las redes de área local en las grandes organizaciones en general recurren a una red troncal de fibra óptica, pero siguen utilizando UTP Cat 5e o uno superior para conectar concentradors o switches con estaciones de trabajo. [11]

Se expondrán a continuación los dos escenarios más relevantes con respecto a este trabajo:

### Backbone serial

Es el tipo más simple de ***backbone***. Se compone de dos o más dispositivos de conectividad, que permiten a las redes estar conectadas entre sí por un solo cable en una cadena. En una red, una conexión en cadena no es más que una serie de dispositivos vinculados. Concentradores y switches a menudo están conectados en cadena para extender una red. [12]

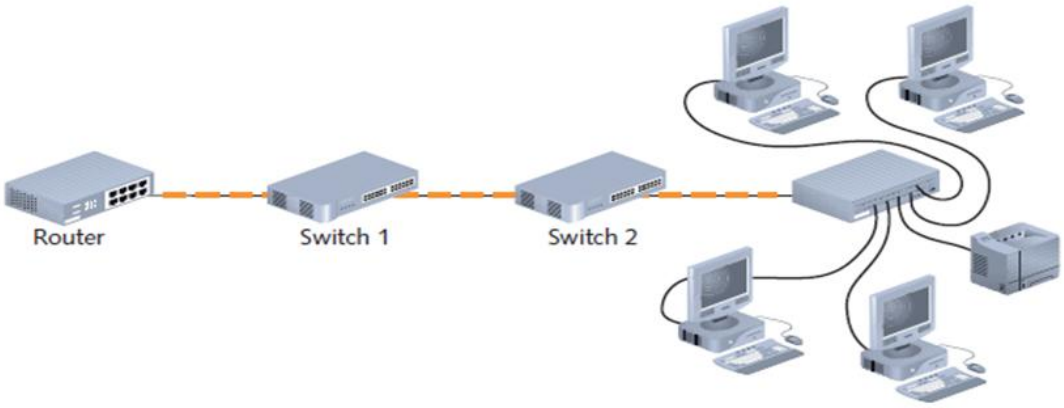


**Figura 2-9.** ***Backbone serial***

**Fuente: Dean, 2009**

### Backbone distribuido

Esta topología consta de un número de equipos de conexión conectados a una serie de dispositivos centrales de conectividad, tales como concentradores (Hubs), conmutadores (Switch) o enrutadores (routers) dispuestos en una forma jerárquica. [13]

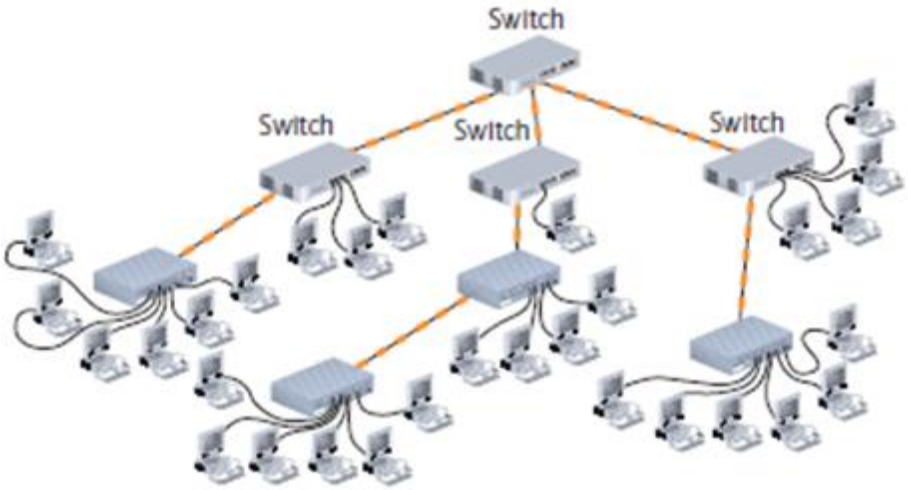


**Figura 2-10 .** ***Backbone distribuido***

**Fuente: Dean, 2009**

### 2.1.3 Aplicaciones y Servicios

La capa de aplicación es la más cercana al usuario y es la que utiliza para interactuar con la red. En ella funcionan los servicios como correo electrónico y VoIP. El administrador de la red en esta capa define también los servicios necesarios para administrar los recursos de la red. A continuación se explican brevemente los servicios relevantes para el diseño referente a las redes que se expondrán en este trabajo.

#### 2.1.3.1 Aplicación DNS

Antes de conocer qué es un servidor de dominio, es importante comprender la definición de **Nombre de Dominio.** Es una denominación entendible por las personas, se asocia con una empresa u otro tipo de organización, como una universidad, organización gubernamental, etc. Un nombre de dominio está representado por una serie de cadenas de caracteres, llamados etiquetas, separadas por

puntos. Cada etiqueta representa un nivel en la jerarquía de nombres de dominio. Por ejemplo, en el nombre de dominio www.google.com, com es el dominio de nivel superior, google es el dominio de segundo nivel, y www es el dominio de tercer nivel también denominado URL. [14]

La aplicación DNS contiene las bases de datos de nombres asociados a direcciones IP y proporcionan esta información a quienes realizan las peticiones. Si un servidor de nombres no puede resolver el nombre de dominio a su dirección IP, pasa la consulta para un servidor de mayor jerarquía.

El servicio DNS está organizado de manera jerárquica. Cuando un servidor DNS no puede resolver la dirección IP del nombre de dominio acude al servidor que está por encima de él en la jerarquía. En el tope de esta jerarquía están los DNS de raíz, ubicados entre trece localidades diferentes a nivel mundial. [15]

La dirección IP del servidor DNS primario de la empresa CANTV de Venezuela es 200.44.32.12.

#### 2.1.3.2 DCHP

Para entender el servicio DHCP es necesario previamente conocer los siguientes conceptos:

**Dirección IP:** es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol)**.**

**Rango servidor DHCP**: está definido por un grupo de direcciones IP en una subred determinada, como por ejemplo de 192.168.0.1 a 192.168.0.254, que el servidor DHCP puede conceder a los clientes.

**Concesión o alquiler de direcciones**: es un período de tiempo durante el cual un equipo cliente puede utilizar una dirección IP asignada.

El protocolo de configuración dinámica de host (DHCP), es un estándar TCP/IP diseñado para simplificar la administración de los clientes de una red. El estándar DHCP permite la asignación dinámica de direcciones IP a los clientes, y otros detalles de configuración tales como la dirección IP de la puerta de enlace o el servidor DNS.

En las redes TCP/IP, el servicio DHCP reduce la complejidad y cantidad de trabajo que debe realizar el administrador para reconfigurar los equipos. Utiliza un modelo cliente-servidor en el que el servidor DHCP mantiene una administración centralizada de las direcciones IP utilizadas en la red. Los clientes compatibles con DHCP podrán solicitar a un servidor DHCP una dirección IP y obtener la concesión del rango en el que opera de entre aquellas que se encuentran libres, como parte del proceso de inicio de red. [16]

### 2.1.3.3 PROXY

**Proxy** es un dispositivo o software que ejecuta una operación en representación de otro, por ejemplo, si un equipo ***X*** requiere un recurso de un equipo ***Y***, lo hará mediante un tercero situado entre los dos llamado ***Z***; de esta manera ***Y*** no estará al tanto que la petición provino inicialmente de ***X***. El *Proxy* Es empleado en distintos ámbitos y con distintas funcionalidades como puede ser seguridad (filtrado), anonimato, proporcionar caché, control de acceso, observación del tráfico, evitar tráfico indeseado, etc.

El servidor Proxy maneja la seguridad en la capa de Aplicación del modelo OSI. Puede utilizarse para registrar el uso de Internet y también para bloquear el acceso sitios a Web.

Los servidores proxy:

- **Funcionan como cortafuegos y como filtro de contenidos.** Son un mecanismo de seguridad implementado por el ISP o los administradores de la red en un entorno de Intranet para desactivar el acceso o filtrar las solicitudes de contenido para ciertos sitios web considerados ofensivos o dañinos para la red y los usuarios.

- **Mejoran el rendimiento.** Guardan en una memoria las páginas web a las que acceden los sistemas de la red durante un cierto tiempo. Cuando un sistema solicita la misma página web, el servidor proxy utiliza la información guardada en la memoria caché en lugar de recuperarla del proveedor de contenidos. De esta forma, se accede con más rapidez a las páginas Web. [17]

#### 2.1.3.4 Proxy Caché

El servidor *Proxy Caché* permite optimizar el uso de ancho de banda, reducir latencias y por lo general hacer un uso más racional de los recursos disponibles.

Un *proxy cache* funciona de la siguiente manera:

En el momento que se realiza una petición a un servidor web, ésta llega al *proxy*, este revisa su cache (en su memoria) para comprobar si dispone de los objetos que se han solicitado. Si los objetos buscados se encuentran en cache, el *proxy* verifica lo siguiente: si no han expirado y si los objetos se corresponden con lo actual.

De ser cierto se produce un ***HIT*** y el sistema envía al cliente los objetos en cuestión. De lo contrario, se produce un ***MISS*** en caché, tras lo cual el proxy descarga los elementos solicitados del servidor web y lo sirve al cliente. [18]

#### 2.1.3.5 Servicio de correo electrónico

El servidor de correo se encargará de gestionar los correos de los usuarios de su dominio o empresa (ejemplo:@supracaracas.com), pudiendo atender miles de correos y definiendo una cantidad ilimitada de buzones de correo electrónico dentro de un mismo dominio.

Cuando un usuario de su dominio envía un correo, primero llega a su servidor de correo que luego lo envía al servidor destinatario utilizando el protocolo SMTP, donde el mensaje queda almacenado en el buzón del destinatario. Cuando el destinatario se conecte al servidor, éste le enviara todos sus mensajes pendientes utilizando los protocolos IMAP, POP, etc. [19]

#### 2.1.3.6 Servicio VoIP

**Voz sobre Protocolo de Internet**. En redes de datos es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando el protocolo IP, esto significa que se envía la señal de voz, en paquetes de datos, en lugar de enviarla a través de circuitos utilizables sólo por telefonía convencional como las redes PSTN. [20]

**Servidor VoIP**

Un servidor VoIP se encarga de la señalización y control de las llamadas IP. El servidor se encarga, mediante diferentes protocolos, de hacer posible una comunicación de voz de calidad aceptable utilizando conmutación de paquetes en una red de datos. Una vez se culmina el proceso de conversión de audio en paquetes de datos, la información viaja mediante una red IP a cualquier persona pueda establecer una llamada de este tipo.

### 2.1.4 Protocolos de Transporte

Los protocolos de transporte se encargan de la comunicación lógica entre procesos de equipos conectados en red. Según la aplicación, los protocolos e transporte pueden ser orientados a conexión o no. Los dos protocolos de transporte que son utilizados en casi todos los casos son TCP y UDP.

#### 2.1.4.1 TCP

El protocolo control de transmisión, de su nombre en inglés Transfer control Protocol (TCP), opera en la capa de transporte del modelo OSI y proporciona servicios confiables de entrega de datos. TCP es un protocolo orientado a la conexión, lo que significa que una conexión debe establecer la comunicación entre los nodos antes de que este protocolo transmita datos.

TCP garantiza, además, la entrega de datos confiable a través de secuenciación y sumas de comprobación. Sin estas medidas, los datos se transmiten de manera indiscriminada, sin comprobar si el nodo de destino se encuentra en línea, por ejemplo, o si los datos se corrompieron durante la transmisión. Finalmente, TCP proporciona control de flujo para asegurar que un nodo no está saturado de datos. [21]

#### 2.1.4.2 UDP

UDP (*User Datagram Protocol*), al igual que TCP, pertenece a la capa de transporte del modelo OSI. Sin embargo, a diferencia de TCP, el UDP es un servicio de transporte no orientado a conexión. En otras palabras, UDP no ofrece ninguna garantía de que los paquetes serán recibidos en la secuencia correcta. De hecho, este protocolo no garantiza que los paquetes serán recibidos en absoluto. Además, no proporciona ninguna comprobación de errores o secuenciación. Sin embargo, la falta de sofisticación del UDP hace que sea más rapido que TCP.

El protocolo UDP puede ser útil en situaciones en las que se exige un gran volumen de datos transferidos rápidamente, como audio en vivo o transmisiones de vídeo a través de Internet. Para estos casos, TCP, con los mecanismos de sumas de comprobación y control de flujo sólo añadiría más sobrecarga a la transmisión. UDP es también más eficiente para llevar mensajes que caben dentro de un paquete de datos. [22]

### 2.1.5 Protocolos de red

En esta etapa se da una introducción a los protocolos que se utilizan en la capa de red, para lógicamente llevar los paquetes de datos desde su origen hasta su destino con éxito. También se exponen los elementos físicos de la red donde se ejecutan estos protocolos y la función que estos realizan.

#### 2.1.5.1 Protocolo IP

IP (Protocolo de Internet), pertenece a la capa de red del modelo OSI. En esta capa los datos se transmiten en paquetes. Un paquete IP contiene la información necesaria para que los Enrutadores puedan transferir datos entre diferentes segmentos

de la LAN. Proporciona información sobre cómo y dónde los datos deben ser entregados, incluyendo la fuente de los datos y direcciones de destino.

IP es un protocolo no confiable, no orientado a conexión, lo que significa que no garantiza la entrega de datos. Sin embargo, protocolos de alto nivel de la suite TCP / IP, utilizan IP para garantizar que los paquetes de datos se entregan a las direcciones correctas. [23]

#### 2.1.5.2 Direccionamiento IP

Una dirección IP es un único número de 32 bits, dividido en cuatro octetos, o conjuntos de ocho bits, que están separados por puntos. Un byte contiene ocho bits, cada octeto es un byte, y así una dirección IP se compone de cuatro bytes.

Una dirección IP contiene dos partes diferentes de información: la red y la de host. Con el primer octeto, se puede determinar la clase de red, en direccionamiento IP tradicional se utilizan tres tipos de clases de red para redes de área local: Clase **A**, Clase **B** y Clase **C**.

Existen Además, direcciones de clase D y clase E, pero se utilizan en casos específicos. Las direcciones de **clase D**, que comienzan con un octeto cuyo valor está comprendido entre **224** y **239**, están reservadas para multidifusión. La IETF (Internet Engineering Task Force) se reserva las direcciones de **clase E**, que comienzan con un octeto cuyo valor está comprendido entre **240** y **254**, para uso experimental. Nunca se debe asignar las direcciones Clase D o Clase E a los dispositivos de la red.

Aunque ocho bits generan **256** combinaciones posibles, sólo los números del **1** al **254** pueden ser utilizados para identificar redes y hosts en una dirección IP. El número **0** está reservado para actuar como un marcador de posición para referirse a un grupo de equipos en una red, por ejemplo, 10.0.0.0 representa todos los dispositivos cuyo primer octeto es 10.

El número 255 está reservado para transmisiones de difusión. Por ejemplo, enviar un mensaje a la dirección 255.255.255.255 envía un mensaje a todos los dispositivos conectados a su segmento de red. En la siguiente tabla se muestra un resumen de las direcciones IP más utilizadas en LANs, con sus respectivas clases. [24]

**Tabla 2-1.** ***Direcciones IPv4 con clase***

| Clase | Primer octeto | Número de redes | Máximo número de host asignables |
|---|---|---|---|
| **A** | **1-126** | **126** | **16.777.214** |
| **B** | **128-191** | **>16.000** | **65.534** |
| **C** | **192-223** | **>2.000.000** | **254** |

### 2.1.5.3 Subneteo

El Subnetting o Subneteo, es una técnica que consiste el proceso de separar una red en varios segmentos definidos lógicamente, o subredes. Las redes son comúnmente subdivididas según las ubicaciones geográficas, por ejemplo, los pisos de un edificio conectados a una LAN, o los edificios conectados por una red WAN, los límites departamentales o tipos de tecnología, por ejemplo, Ethernet o Token Ring. Cuando se lleva a cabo la división en subredes, el tráfico de cada subred se separa del otro. Un administrador de red puede separar el tráfico para lograr lo siguiente:

**Mejorar la seguridad**. Las subredes deben estar conectadas a través de Enrutadores u otros dispositivos capa 3. Estos dispositivos no retransmiten tramas de entrada a todos los demás nodos en el mismo segmento (como un concentrador o switch hace). En su lugar, envían tramas sólo cuando sea necesario para llegar a su destino. Debido a que cada trama no es retransmitida en todos los puertos del

enrutador, la posibilidad de que un nodo pueda toparse con las transmisiones del otro nodo se reduce.

**Mejorar el desempeño**. Por la misma razón que la división en subredes mejora la seguridad, también mejora el rendimiento de la red. Cuando los datos son selectivamente retransmitidos, las transmisiones innecesarias se mantienen a un mínimo. El subneteo es útil para limitar la cantidad de tráfico de difusión ***(broadcast***) y por lo tanto, la cantidad de posibles colisiones en redes Ethernet, al disminuir el tamaño de cada dominio de difusión. Se logra un uso más eficiente de los resultados de ancho de banda y eso conlleva a un mejor rendimiento global de la red.

**Simplificar solución de problemas**. Si un administrador de red puede subdividir la red de una organización, de acuerdo a la geografía, o de los nodos en la oficina del centro, oficina del lado oeste, y la oficina del lado este de su compañía. Si se supone que un día la red tiene problemas para transmitir datos sólo a un grupo determinado de direcciones IP en algún nodo.

Para solucionar los problemas, en lugar de examinar toda la red por errores o cuellos de botella, el administrador de la red sólo tiene que ver las transmisiones defectuosas que están asociadas a las direcciones de la subred en el nodo afectado. [25]

**Direccionamiento con Clases**

En IPv4 el direccionamiento con clases se adhiere a las diferencias de clase de red. En este tipo de direccionamiento, sólo son reconocidas las direcciones Clase A, Clase B y Clase C. Es importante recordar que todas las direcciones IPv4 consisten en información de red e información de host.

En direccionamiento con clases, la parte de información de red de una dirección IPv4 (el ID de red) está limitada a los primeros 8 bits de una dirección

Clase A, en los primeros 16 bits de una dirección Clase B, y en los primeros 24 bits en una dirección de clase C.

La información de Host está contenida en los últimos 24 bits para una dirección de clase A, en los últimos 16 bits de una dirección Clase B, y en los últimos 8 bits en una dirección de clase C. [26]

**Máscara de subred**

El subneteo en IPv4, depende del uso de máscaras de subred para identificar cómo está dividida la red. Una máscara de subred indica donde la información de red se encuentra en una dirección IPv4.

Los bits "1" en una máscara de subred indican los bits correspondientes, en una dirección IPv4, a la información de la red. Los bits "0" en una máscara de subred indican los bits que contienen información de host. Cada clase de red está asociada con una máscara de subred predeterminada, como se muestra en la Tabla 2-2.

Por ejemplo, por defecto, el primer octeto de una dirección Clase A (o de ocho bits) representa la información de la red y se compone de todos los "1". Cabe destacar que un octeto integrado por todos los "1s" en notación binaria es igual a **255** en notación decimal. Un octeto integrado por todos los "0" en notación binaria es igual a "0" en notación decimal. Esto significa que si se trabaja en una red cuyos host están configurados con una subred máscara de 255.0.0.0, se sabe que la red utiliza direcciones de clase A y además que no está utilizando subredes, ya que 255.0.0.0 es la máscara de subred predeterminada para una red de clase A.

**Tabla 2-2.** ***Mascaras de subred***

| Clase | Mascara de subred por defecto (binario) | Número de bits utilizados para la información de red | Mascara de subred por defecto (decimal) |
|---|---|---|---|
| **A** | **11111111 00000000 00000000 00000000** | **8** | **255.0.0.0** |
| **B** | **11111111 11111111 00000000 00000000** | **16** | **255.255.0.0** |
| **C** | **11111111 11111111 11111111 00000000** | **24** | **255.255.255.0** |

Es posible calcular el ID de la red de un host dada su dirección IPv4 y la máscara de subred, para ello se sigue un proceso lógico de combinar los bits conocidos como AND. Un bit con un valor de 1, más otro bit con un valor de 1 da como resultado un 1. Un bit con un valor de 0, con cualquier otro bit es un 0. [27]

A continuación se muestra un ejemplo de esta operación.

**Tabla 2-3.** ***Ejemplo cálculo dirección de red***

| Dirección IP | 11000111 | 01000100 | 00100010 | 01111111 | 199.34.89.127 |
|---|---|---|---|---|---|
| **Mascara de subred** | **11111111** | **11111111** | **11111111** | **00000000** | **255.255.255.0** |
| **ID de la red** | **11000111** | **01000100** | **00100010** | **00000000** | **199.34.89.0** |

### Técnicas de Subneteo con máscara de red sin clase

Las Técnicas de subneteo sin clase no utilizan reglas de direccionamiento con clases IPv4. Para crear subredes, algunos de los bits de una dirección IP, que en el direccionamiento con clases representan la información de host, se cambian para representar la información de la red en su lugar. Al hacer que los bits que anteriormente se utilizaban para representar la información de host ahora representen la información de la red, se reduce el número de bits disponibles para la identificación de los hosts. En consecuencia, se reduce el número de direcciones de host utilizables por subred.

El número de hosts y subredes disponibles después de la división en subredes, se relaciona con el número de bits de información de host que usa para obtener información de la red. La Tabla 2-4 muestra el número de subredes y hosts que pueden ser creados por la división en subredes de una red Clase B. Observe la gama de máscaras de subred que se pueden utilizar en lugar de la máscara de subred predeterminada de Clase B 255.255.0.0. También se comparan la cantidad de hosts por subred a los 65.534 hosts disponibles en una red de clase B que no utiliza subredes. [28]

**Tabla 2-4.** ***Subneteo direcciones clase B***

| Máscara de subred (binario y decimal) | Número de subredes | Número de host por subred |
|---|---|---|
| **11111111 11111111 11000000 00000000 ó 255.255.192.0** | **2** | **16.382** |
| **11111111 11111111 11100000 00000000 ó 255.255.224.0** | **6** | **8190** |
| **11111111 11111111 11110000 00000000 ó 255.255.240.0** | **14** | **4094** |
| **11111111 11111111 11111000 00000000 ó 255.255.248.0** | **30** | **2046** |
| **11111111 11111111 11111100 00000000 ó 255.255.252.0** | **62** | **1022** |
| **11111111 11111111 11111110 00000000 ó 255.255.254.0** | **126** | **510** |
| **11111111 11111111 11111111 00000000 ó 255.255.255.0** | **254** | **254** |
| **11111111 11111111 11111111 10000000 ó 255.255.255.128** | **510** | **126** |
| **11111111 11111111 11111111 11000000 ó 255.255.255.192** | **1022** | **62** |
| **11111111 11111111 11111111 11100000 ó 255.255.255.224** | **2046** | **30** |
| **11111111 11111111 11111111 11110000 ó 255.255.255.240** | **4094** | **14** |
| **11111111 11111111 11111111 11111000 ó 255.255.255.248** | **8190** | **6** |
| **11111111 11111111 11111111 11111100 ó 255.255.255.252** | **16.382** | **2** |

La fórmula para determinar cómo modificar la máscara de subred por defecto es:

$$2^n - 2 = Y$$

Donde n es igual al número de bits en la máscara de subred que debe ser cambiado de 0 a 1 y Y es igual a la cantidad de subredes que se derivan.

### 2.1.5.4 Traducción de direcciones IP

Prácticamente todas las redes LAN y WAN de negocios son redes privadas. En las redes privadas, utilizar las direcciones IP privadas permite a los

administradores de red más flexibilidad en la asignación de direcciones. Los clientes en una red pueden utilizar cualquier esquema de direccionamiento IP, sin importar si es reconocido como legítimo por las autoridades de Internet. Pero tan pronto como los clientes necesitan conectarse a Internet, debe tener una dirección IP pública para intercambiar datos.

Cuando la transmisión del cliente llega a la puerta de enlace predeterminada, la puerta se abre el paquete IP y sustituye la dirección IP privada por una dirección IP reconocida por internet. Este proceso se conoce como **NAT (traducción de direcciones de red).** Unos pocos tipos de **NAT** están disponibles para los administradores de red.

Una de las razones para el uso de la traducción de direcciones es superar las limitaciones de una baja cantidad de direcciones públicas IPv4. En la actualidad una pequeña empresa con 25 hosts, por ejemplo, sólo puede ser capaz de alquilar una dirección IP desde su ISP. Sin embargo, la empresa aún necesita permitir que todos sus hosts tengan acceso a Internet. Con la traducción de direcciones, los 25 hosts pueden compartir una única dirección IP enrutable en Internet.

Otra razón para el uso de la traducción de direcciones es añadir una cantidad adicional de seguridad a una red privada cuando está conectada a una red pública. Debido a que durante la transmisión se le asigna una nueva dirección IP cada vez que se llega a la esfera pública, los que están fuera de una organización no puede rastrear el origen de la transmisión al nodo de red específico que lo envió. Sin embargo, la dirección IP asignada a una transmisión por la puerta de enlace debe ser una dirección IP de Internet autorizada, por lo que se puede remontar de nuevo a la organización que arrendó la dirección.

Una tercera razón para utilizar la traducción de direcciones es permitir que un administrador de red pueda desarrollar su propio esquema de direccionamiento de red que no se ajusta a un esquema determinado por la ICANN.

Si se han alquilado al menos 50 direcciones IP válidas de la ISP, se puede asignar a cada cliente una dirección IP correspondiente para su uso en Internet. Este tipo de traducción de direcciones se conoce como **SNAT (traducción de dirección de red estática)**. Se considera estático, ya que cada cliente está asociado con una dirección IP privada y una dirección IP pública que nunca cambia. SNAT es útil para operar un servidor de correo, por ejemplo, cuya dirección debe seguir siendo la misma para que los clientes puedan llegar a él en cualquier momento.

Suponiendo que no se requiere que todos los clientes de una red se conecten a Internet en todo momento y se decide alquilar sólo ocho direcciones IP de su ISP, se debe configurar la puerta de enlace para traducir las direcciones privadas a las direcciones IP que se pueden utilizar en Internet.

Cada vez que un cliente intenta acceder a Internet, la puerta de enlace sustituirá su campo de dirección de origen en el paquete con una de las ocho direcciones IP públicas. Debido a que cualquier dirección IP válida en Internet podría ser asignada a cualquier transmisión de salida del cliente, esta técnica se conoce como **DNAT (Traducción de Dirección de red dinámica).** También puede ser llamado enmascaramiento IP.

Es posible preguntarse cómo un host de Internet puede responder a un cliente en una red privada que utiliza DNAT, si todos los clientes de red comparten un pequeño grupo de direcciones. De hecho, para realizar DNAT, una puerta de enlace realiza **PAT (Traducción de dirección de puerto)**. Con PAT cada sesión de cliente con un servidor en Internet se le asigna un número de puerto TCP separado. Cuando el cliente emite una solicitud al servidor, su dirección de origen del paquete incluye este número de puerto.

Cuando el servidor responde a Internet, su dirección de destino del paquete incluye el mismo número de puerto. Esto permite que la puerta de enlace pueda enviar la respuesta al cliente apropiado. PAT es el tipo más común de traducción de direcciones utilizado en pequeñas oficinas y redes domésticas. [29]

#### 2.1.5.5 Enrutadores

Un enrutador típico posee un procesador interno, un sistema operativo, memoria, un conmutador de entradas y salida para diferentes tipos de interfaces de red y por lo general, una interfaz de gestión de la consola.

Un enrutador es un dispositivo de conectividad multipuerto que transmite los datos entre diferentes redes. Los enrutadores pueden integrar redes LAN y WAN, funcionando a diferentes velocidades de transmisión y permitiendo el uso de una variedad de protocolos.

Cuando un enrutador recibe un paquete entrante, lee el encabezado donde están las direcciones IP. Basándose en esto, se determina a qué red el paquete debe ser entregado. A continuación, se determina la ruta más corta a esa red y por último, se reenvía el paquete al siguiente salto en ese camino.

Los Enrutadores operan en la capa de red (capa 3) del modelo OSI. Ellos pueden ser equipos configurados para realizar servicios de enrutamiento. Cabe recordar que los protocolos de capa de red, direccionan los datos de un segmento o tipo de red a otra. El direccionamiento lógico utilizando protocolos como IP, también ocurre en esta capa. Por consiguiente, a diferencia de los puentes y los switches de Capa 2, los enrutadores dependen del protocolo.

En otras palabras, éstos deben ser diseñados o configurados para reconocer un protocolo de capa de red determinado, antes de que se pueda reenviar datos transmitidos usando dicho protocolo. En términos generales, los enrutadores son más lentos que los Switches o puentes, porque se toman el tiempo para interpretar la información de la capas 3.

Los Enrutadores tradicionales en redes LAN están siendo reemplazados por conmutadores de nivel 3 que apoyan las funciones de enrutamiento. Sin embargo, a pesar de la competencia de los ***switches de Capa 3***, los enrutadores están encontrando nichos en aplicaciones especializadas tales como la vinculación de grandes nodos de Internet o el servicio de llamadas telefónicas digitalizadas.

La fuerza del enrutador reside en su inteligencia. No sólo puede hacer seguimiento de las ubicaciones de ciertos nodos de la red, tal como los Switch, sino que también puede determinar la ruta más rápida entre dos nodos.

Por esta razón, y porque se pueden conectar diferentes tipos de redes, los enrutadores son dispositivos de gran alcance, indispensables en grandes redes LAN y WAN. [30]

### 2.1.5.6 Enrutamiento estático y dinámico

Los enrutadores pueden utilizar uno de dos métodos para dirigir los datos de la red: enrutamiento estático o dinámico. El ***enrutamiento estático*** es una técnica en la que un administrador de red programa un enrutador para utilizar rutas específicas entre los nodos.

Debido a que no tiene en cuenta la congestión de red, ocasionalmente este tipo de enrutamiento genera fallos en la conexión, por lo no es óptimo. Si un enrutador o un segmento conectado a un enrutador se cambia de lugar, el

administrador de la red debe volver a programar las tablas del enrutador estático. El enrutamiento estático requiere la intervención humana, por lo que es menos eficiente y preciso que el encaminamiento dinámico.

El ***enrutamiento dinámico***, por otra parte, calcula automáticamente la mejor ruta entre dos nodos y acumula dicha información en una tabla de enrutamiento. Si la congestión o fallos afectan a la red, un enrutador mediante enrutamiento dinámico puede detectar los problemas y redirigir los paquetes a través de un camino diferente.

Como parte del enrutamiento dinámico, de forma predeterminada, cuando se agrega un enrutador a una red los protocolos de enrutamiento proceden a actualizar sus tablas de enrutamiento. La mayoría de las redes utilizan principalmente enrutamiento dinámico, pero pueden incluir algún enrutamiento estático para indicar por ejemplo, un enrutador de salida por defecto. [31]

**Protocolos de enrutamiento**

Encontrar la mejor ruta que deban tener los datos en la red es una de las funciones más valoradas y sofisticadas realizadas por un enrutador. El mejor camino se refiere a la ruta más eficaz desde un nodo en una red a otra. El mejor camino en una situación particular depende del número de saltos entre los nodos, la actividad de la red actual, los vínculos no disponibles, la velocidad de la red de transmisión, y la topología.

Para determinar la mejor ruta, los enrutadores se comunican entre sí a través de los protocolos de enrutamiento. Se debe tener en cuenta que los protocolos de enrutamiento no son los mismos que los protocolos enrutables, como TCP / IP, a pesar de que los protocolos de enrutamiento pueden superponerse sobre los protocolos enrutables. Los protocolos de enrutamiento sólo se utilizan para recopilar datos sobre el estado actual de la red y para contribuir a la selección de los mejores

caminos. A partir de estos datos, los enrutadores crean tablas de enrutamiento, que actúan como una especie de hoja de ruta para el reenvío de paquetes en el futuro.

Además de su capacidad para encontrar el mejor camino, un protocolo de enrutamiento puede caracterizarse de acuerdo a su tiempo de convergencia, éste tiempo es el que toma un enrutador para reconocer una mejor ruta en el caso de cambio o de caída de la red. Los protocolos más comunes de enrutamiento son: RIP, RIPv2, BGP, OSPF y EIGRP.

**RIP** (*Routing Information Protocol*). Es un protocolo de enrutamiento que utiliza un algoritmo de enrutamiento conocido como vector distancia, es el más antiguo de los protocolos de enrutamiento. El factor que RIP toma en cuenta para su enrutamiento, es sólo el número de saltos entre los nodos a la hora de determinar la mejor ruta de un punto a otro. No tiene en cuenta la congestión de la red o velocidad de enlace. RIP es un protocolo de enrutamiento interior, lo que significa que se utiliza en interiores o enrutadores frontera. Los enrutadores que utilizan RIP difunden sus tablas de enrutamiento cada 30 segundos para otros enrutadores. Esta radiodifusión genera tráfico de red excesivo, especialmente si un gran número de rutas existen.

RIP evita que los bucles de enrutamiento continúen indefinidamente, al limitar el número de saltos que un paquete puede tomar entre su fuente y su destino a 15. Si el número de saltos en una ruta de acceso supera los 15 saltos, el destino de la red se considera inalcanzable. Es por esto que RIP no funciona bien en entornos de red muy grandes en las que los datos pueden tener que viajar a través de más de 15 enrutadores para llegar a su destino (por ejemplo, en Internet). Además, en comparación con otros protocolos de enrutamiento, RIP es más lento y menos seguro.

**RIPv2** (*Routing Information Protocol Version 2*), este protocolo genera menos tráfico de difusión y las funciones son más seguras que RIP. Aún así, RIPv2

no puede superar los 15 saltos y se usa con menos frecuencia que algunos protocolos de enrutamiento.

Un protocolo de enrutamiento basado en el algoritmo vector-distancia adecuado para redes **WAN** es **BGP** (*Border Gateway Protocol*). A diferencia de RIP, BGP se comunica mediante mensajes específicos para BGP, que viajan entre los enrutadores sobre sesiones TCP.

Utilizando BGP, los enrutadores pueden determinar las mejores rutas de acceso basado en muchos factores diferentes. Además, los administradores de red pueden configurar BGP para seguir políticas que podrían, por ejemplo, evitar un enrutador determinado o instruir a un grupo de enrutadores para preferir una ruta en particular sobre otras rutas disponibles. BGP es el protocolo de enrutamiento de preferencia para el tráfico de Internet, y se usa en enrutadores de borde y enrutadores exteriores pero no en enrutadores interiores.

Un protocolo de enrutamiento basado en el algoritmo de estado-enlace es el que permite que los enrutadores en una red puedan compartir información, luego de cada uno determine de forma independiente la mejor ruta entre él y el nodo de destino del paquete. Por el contrario, los protocolos de enrutamiento vector-distancia de los enrutadores, dependen de sus vecinos para información de la ruta de datos.

**OSPF** (*Open Shortest Path First*) es un protocolo de enrutamiento basado en el algoritmo de estado-enlace utilizado en los enrutadores de interior o borde. Se presenta como una mejora a RIP y puede coexistir con RIP (o RIPv2) en una red. A diferencia de RIP, OSPF no impone límites de saltos en una vía de transmisión. Además, OSPF utiliza un algoritmo más complejo que RIP, para determinar las mejores rutas.

En condiciones óptimas de la red, la mejor ruta es el camino más directo entre dos puntos. Si los niveles de exceso de tráfico o una interrupción impiden a los datos seguir el camino más directo, un enrutador puede determinar que el camino más eficiente en realidad pasa a través de enrutadores adicionales.

Debido a que OSPF es un protocolo de enrutamiento de estado-enlace, cada enrutador que ejecuta OSPF mantiene una base de datos de enlaces a los otros enrutadores. Si OSPF aprende de la falla de un enlace dado, el enrutador puede rápidamente calcular una ruta alternativa. Este cálculo requiere más memoria y potencia de CPU que RIP, pero mantiene el ancho de banda de red a un mínimo y ofrece un tiempo de convergencia muy rápida, a menudo invisible para los usuarios.

OSPF es compatible con todos los enrutadores modernos. Por lo tanto, se utiliza comúnmente en las redes LAN que se basan en una mezcla de enrutadores de diferentes fabricantes.

Algunos protocolos de enrutamiento reflejan características tanto del estado-enlace como de protocolos de enrutamiento vector-distancia, y se conocen como protocolos de enrutamiento híbridos.

El ejemplo más popular es **EIGRP** (*Enhanced Interior Gateway Routing Protocol*). Este protocolo de enrutamiento utilizado en los enrutadores de interior o de borde, se desarrolló en la década de 1980 por Cisco Systems. Tiene un tiempo de convergencia rápido y una sobrecarga de la red baja y es más fácil de configurar y menos intensivo en el uso del CPU que OSPF.

EIGRP también ofrece los beneficios de apoyar múltiples protocolos y limitar el tráfico innecesario en la red entre los enrutadores. Tiene capacidad para redes muy grandes y heterogéneas, pero *sólo es compatible con los enrutadores de Cisco*. [32]

### 2.1.6 Acceso a La Red

En el acceso a la red se presentan algunos de los protocolos que permiten la comunicación en esta capa, además se exponen los dispositivos físicos y su funcionamiento.

#### 2.1.6.1 Protocolo Ethernet

Ethernet es una tecnología de red desarrollada originalmente por Xerox en la década de 1970 y posteriormente mejorada por Digital Equipment Corporation (DEC), Intel y Xerox (DIX). Esta tecnología flexible puede funcionar en una variedad de medios de red y ofrece un rendimiento excelente a un coste razonable. Ethernet es la tecnología de red más popular utilizada en LANs modernas y ha evolucionado a través de muchas variaciones; además su velocidad y fiabilidad siguen mejorando. Como resultado de esta historia, es compatible con muchas diferentes versiones. Sin embargo, todas las redes Ethernet tienen al menos una cosa en común: su método de acceso, que es conocido como ***CSMA/CD***. [33]

**CSMA/CD**

Para la siguiente definición de CSMA/CD es necesario previamente conocer el siguiente concepto.

**NIC:** Network Interface Card (Tarjeta de interfaz de red). Es el hardware que sirve para transmitir y recibir información. Este dispositivo conecta la computadora u otro equipo de red con el medio físico. Hoy en día cada vez son más los equipos que disponen de interfaz de red, principalmente Ethernet, incorporadas.

Para entender Ethernet, es necesario comprender CSMA / CD. Todas las redes Ethernet, independientemente de su velocidad, utilizan un método de acceso

llamado CSMA/CD (Acceso múltiple por detección de portadora con detección de colisiones).

El término ***detección de portadora***, se refiere al hecho que las NIC de Ethernet escuchan a la red y esperan hasta que se detecta que no hay otros nodos transmitiendo datos a través del canal, para comenzar a transmitir.

El término ***acceso múltiple***, se refiere al hecho que varios nodos Ethernet se pueden conectar a una red y monitorear el tráfico, o acceder a los medios de comunicación, simultáneamente.

En CSMA / CD, cuando un nodo quiere transmitir datos primero debe acceder a los medios de transmisión y determinar si el canal está libre. Si el canal no está libre, espera y comprueba nuevamente después de un período breve de tiempo. Si el canal está libre, el nodo transmite sus datos. Cualquier nodo puede transmitir datos después de que se determina que el canal está libre.

Si dos nodos comprueban simultáneamente el canal, y determinan que está libre y comienzan a transmitir, las transmisiones interfieren entre sí, lo que se conoce como una colisión de paquetes. La última parte de CSMA / CD, es el término ***detección de colisiones***, se refiere a la manera en que responden los nodos ante una colisión. En el caso de una colisión, la red lleva a cabo una serie de pasos conocidos como la rutina de detección de colisiones. Si la NIC de un nodo determina que sus datos se han involucrado en un incidente, inmediatamente deja de transmitir.

A continuación, realiza un proceso llamado ***jamming***; la NIC emite una secuencia especial de 32-bit que indica al resto de los nodos de la red que su transmisión anterior fue defectuosa y que esos datos no son válidos. Después de esperar, la NIC determina si el canal está disponible de nuevo, y si lo está, la NIC retransmite sus datos.

### 2.1.6.2 Redes metropolitanas con Ethernet

Metro Ethernet (ME) es un diseño de red que permite conexiones de banda ancha en redes privadas, además ofrece servicios necesarios de transporte de datos, tales como internet o conexiones a lugares remotos. En la actualidad Metro Ethernet es el servicio que más frecuentemente ofrecen los proveedores, para interconectar LANs que se encuentran a grandes distancias dentro de una ciudad.

Este tipo de red cubre un área metropolitana, y está basada en el estándar Ethernet. Se utiliza comúnmente como red de acceso, conectando las empresas a una red de área extensa como Internet.

Una red Metro Ethernet está conformada por dispositivos Capa 2 y 3 como concentradors, Switches y Enrutadores, conectados a través de fibra óptica. Las topologías utilizadas pueden ser anillo, estrella, mallada o incluso una combinación de estas. ME es una red jerárquica, que contiene capa de núcleo, distribución y acceso.

El núcleo en la mayoría de las ME es un backbone IP/MPLS, pero podría ser también formas nuevas de transporte Ethernet con velocidades de 10Gbps o 100Gbps. Un modelo básico de servicio ME, está compuesto por una red que funciona bajo switches ME, ofrecida por un proveedor de servicios, donde el acceso de los usuarios a la red, se realiza mediante equipos de los clientes CEs (Customer Equipoment), que se conectan a través de UNIs (User Network Interface) a velocidades de 10Mbps, 100Mbps 1Gbps o 10 Gbps.

ME es también una plataforma multiservicio, ya que soporta una amplia gama de aplicaciones y servicios, contando con mecanismos que incluyen soporte a tráfico RTP (tiempo real), como puede ser telefonía IP y Video IP.

Para una empresa con múltiples ubicaciones en un área metropolitana, se pueden lograr conexiones punto a punto u otro tipo de conexión, mediante una red ME la cual proporciona velocidades desde 10Mbps a 1Gbps, más soporte para 100BaseTX y 1000BaseLX. Una red ME permite a una empresa conectar sus sucursales como si fueran una sola LAN.

Debido a que la mayoría de las empresas utiliza actualmente Ethernet en su entorno de red, ME no requiere de grandes cambios para las interconexiones. Ésta utiliza extensiones familiares de la tecnología LAN de Ethernet y se integra perfectamente con las redes Ethernet y FastEthernet. [34]

#### 2.1.6.3 VPN

VPN (Virtual Private Network) son redes de área amplia definidas lógicamente sobre los sistemas públicos de transporte, de manera tal que solo permiten el acceso a usuarios autorizados. El tráfico en una red privada virtual está aislado del resto del tráfico en la red del operador.

Dos consideraciones importantes a la hora de diseñar una VPN son la interoperabilidad y la seguridad. Una VPN puede llevar todo tipo de datos de manera privada a través de cualquier tipo de conexión, para ello protocolos especiales de VPN encapsulan a los paquetes en un proceso conocido como efecto túnel.

Se puede decir que estos protocolos crean la conexión virtual, o un túnel, entre dos nodos VPN. Un punto final del túnel es el cliente y el otro extremo puede ser un dispositivo de conectividad, por ejemplo, un enrutador, un firewall o un servidor de acceso remoto que permite a los clientes conectarse a la red. [35]

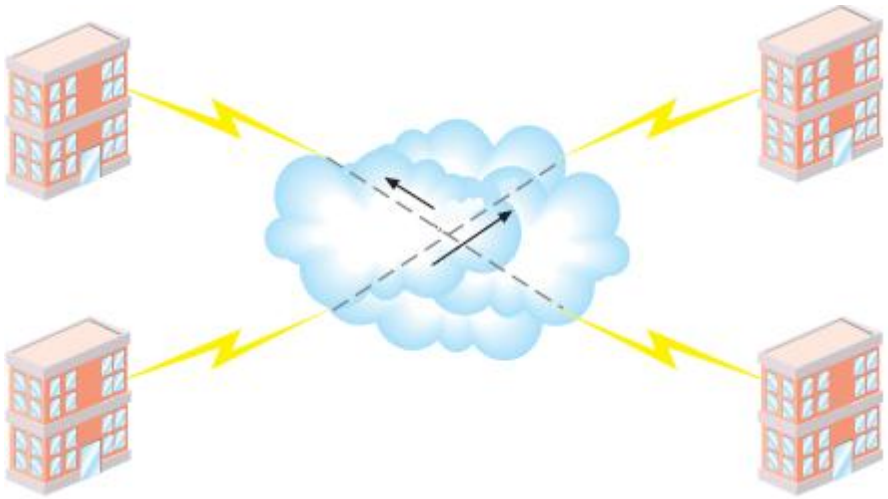

**Figura 2-11.** ***Diagrama VPN***

### 2.1.6.4 Switches

También llamados conmutadores o interruptores, los switches son dispositivos de conectividad que pueden subdividir una red en pequeñas partes lógicas, o segmentos. Los switches convencionales operan en la capa de enlace de datos del modelo OSI, mientras que los más modernos pueden funcionar en la capa 3 o incluso en la capa 4. Al igual que los puentes, los switches interpretan la información de la dirección física de los dispositivos (MAC).

La mayoría de los interruptores han de tener al menos un procesador interno, un sistema operativo, memoria, y varios puertos que permiten a otros nodos conectarse a él.

Debido a que tienen varios puertos, los switches pueden hacer un mejor uso del ancho de banda y ser más rentables que los puentes. Cada puerto del switch actúa como un puente, y cada dispositivo conectado a un interruptor recibe su propio canal dedicado. En otras palabras, un interruptor puede activar un canal compartido en varios canales.

Desde la perspectiva de Ethernet, cada canal dedicado representa un dominio de colisión. Debido a que un interruptor limita el número de dispositivos en un dominio de colisión, limita las posibilidades de que éstas ocurran. Los interruptores han sido históricamente utilizados para reemplazar concentradores y aliviar la congestión de tráfico en grupos de trabajo de redes LAN.

Algunos administradores de red han sustituido a los enrutadores troncales con Switches, estos proporcionan por lo menos dos ventajas: mayor seguridad y mejor rendimiento. Por su naturaleza, los conmutadores proporcionan mayor seguridad que muchos otros dispositivos, ya que pueden aislar el tráfico de un dispositivo del tráfico de otros. Y como conmutadores proporcionan canales separados para todos los dispositivos, mejorando así el rendimiento de la red.

Las aplicaciones que transfieren una gran cantidad de tráfico y son sensibles a las demoras, como las aplicaciones de videoconferencia, se benefician de la utilización plena de la capacidad del canal.

Además de mejorar el uso del ancho de banda en comparación con los dispositivos como concentradores, los switches pueden crear VLANs, de manera tal que la red logra aislar los dispositivos que así lo requieran.

**STP**

Mediante el protocolo STP se deshabilitan virtualmente los puertos que generan loops, haciendo posible la conexión de conexiones de redundancia sin que estas generen errores en la comunicación.

Este protocolo puede adaptarse a los cambios en la red. Por ejemplo, si un Switch se elimina de la red o presenta alguna falla, STP volverá a calcular las mejores rutas de datos entre los Switch restantes y así los datos podrán alcanzar su destino.

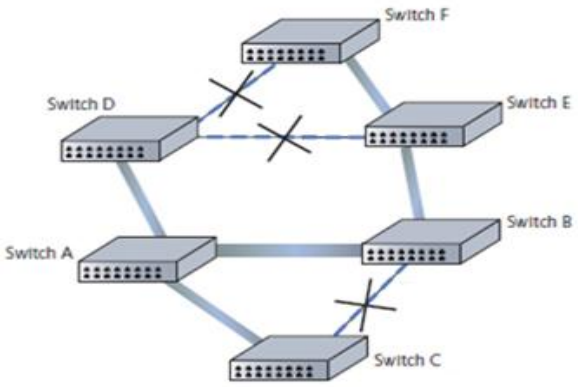


**Figura 2-12.** ***Caminos de datos seleccionado por STP***

**Fuente: Dean, 2009**

### VLANs

VLANs o redes virtuales de área local, son redes lógicamente separadas dentro de una red, mediante la agrupación de puertos en un dominio de ***broadcast*** o difusión. Un ***dominio de broadcast*** es una combinación de puertos que componen un segmento de capa 2. Los puertos en un dominio de broadcast dependen de un dispositivo de capa 2, tal como un switch, para transmitir los datos. En el contexto de las redes TCP / IP, un ***dominio de broadcast*** también se conoce como una ***subred***.

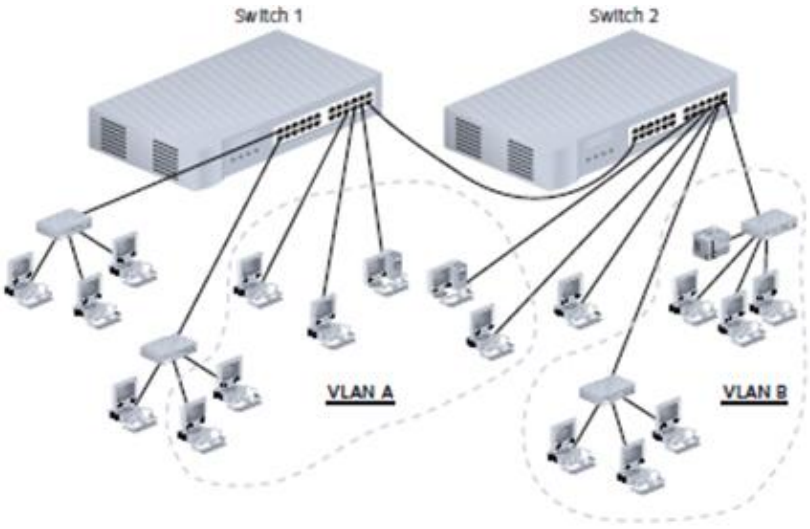


**Figura 2-13.** ***Ejemplo de VLANs***

**Fuente: Dean, 2009**

### 2.1.6.5 Red física

Existen normas y estándares que se deben cumplir a la hora de realizar la conexión física de una red, de manera de garantizar que todas las redes pueden interconectarse entre si y que exista mayor fiabilidad en la entrega de la información.

**Estándares Ethernet**

Los estándares para Ethernet, indican características como métodos de codificación, longitud del segmento y requisitos del cableado, para obtener un rendimiento máximo en la comunicación. A continuación se enuncian algunos de estos.

**10Base-T**.En 10Base-T, el 10 representa su velocidad máxima de 10 Mbps, el término Base indica que se utiliza la transmisión de banda base, y la T representa el medio que utiliza que es par trenzado. En una red Ethernet 10Base-T, un par de hilos en el cable UTP se utiliza para la transmisión, mientras que un segundo par de cables se utiliza para la recepción. Estos dos pares de cables permiten a 10Base-T proporcionar transmisión *full-duplex*. Una red 10Base-T requiere cable UTP Cat. 3 o superior.

10Base-T sigue la regla 5-4-3 de las redes. Esta norma establece que, entre dos nodos de comunicación la red no puede contener más de cinco segmentos de red conectados por cuatro dispositivos de repetición, y al menos dos deben estar despoblados. La distancia máxima en un segmento 10BASE-T es de 100 metros. Para ir más allá de esa distancia, los segmentos Ethernet deben estar conectados mediante concentradores o conmutadores adicionales para formar topologías más complejas.

Los dispositivos se pueden conectar a una distancia total entre los nodos de comunicación de 500 metros. En la figura 2-14 se muestra un ejemplo de esta distancia máxima; *entre la estación de trabajo A y B puede haber máximo 500 m.*

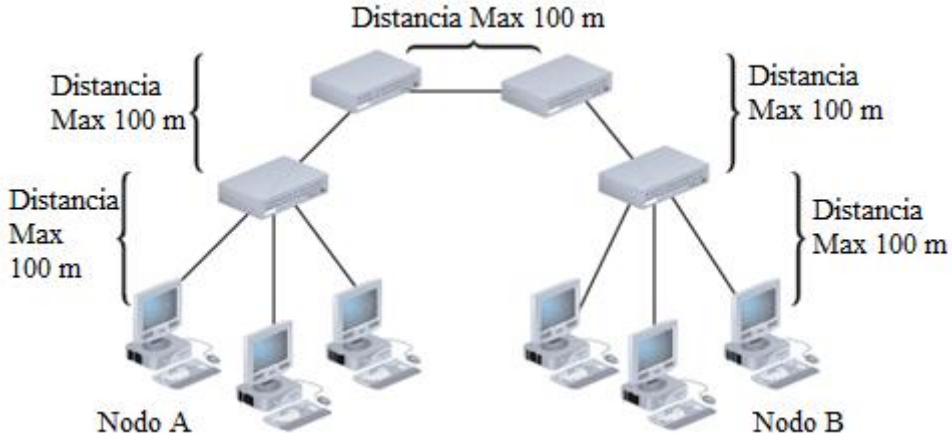


**Figura 2-14.** ***Red 10Base-T***

**Fuente: Dean, 2009**

**100Base-T** (Fast Ethernet). Como las redes se expandieron y manejan tráfico más pesado, Ethernet de 10-Mbps demostró ser un cuello de botella. La necesidad de mayor velocidad en LANs, y la posibilidad de utilizar la misma infraestructura que 10Base-T fue concebido 100Base-T, también conocido como Fast Ethernet. 100Base-T, especificado en el estándar ***IEEE 802.3u***, permite a LANs funcionar a una velocidad de transferencia de 100 Mbps, diez veces más de la prevista por 10Base-T, sin necesidad de una importante inversión en nuevas infraestructuras.

100Base-T utiliza la transmisión de banda base y la misma topología que 10Base-T. También se utilizan conectores modulares **RJ-45**. Dependiendo del tipo de tecnología 100Base-T utilizada, puede requerir cable UTP Cat 3, Cat 5, o superior.

Como con 10Base-T, los nodos en una red 100Base-T están configurados en una topología de estrella. Sin embargo, a diferencia de redes Ethernet de 10-Mbps, las redes con 100Base-T no siguen la regla 5-4-3. Debido a sus requerimientos de respuesta más rápida, los nodos deben estar aún más cerca para evitar errores en la transferencia de datos

Las configuraciones utilizando el estándar 100Base-T, pueden soportar un máximo de tres segmentos de red conectados con dos dispositivos de repetición. Cada longitud de segmento está limitada a 100 metros. Por lo tanto, la longitud máxima entre los nodos se limita a 300 metros, como puede verse en la figura 2-15.

**100Base-T** requiere cable UTP **Cat 5** o superior. En el cable, utiliza los mismos dos pares de hilos para transmitir y dos pares para recibir datos que 10Base-T. Por lo tanto, como 10Base-T, 100Base-TX es también capaz de transmisión full-duplex lo cual potencialmente puede duplicar el ancho de banda efectivo de una red 100Base-T a 200 Mbps.

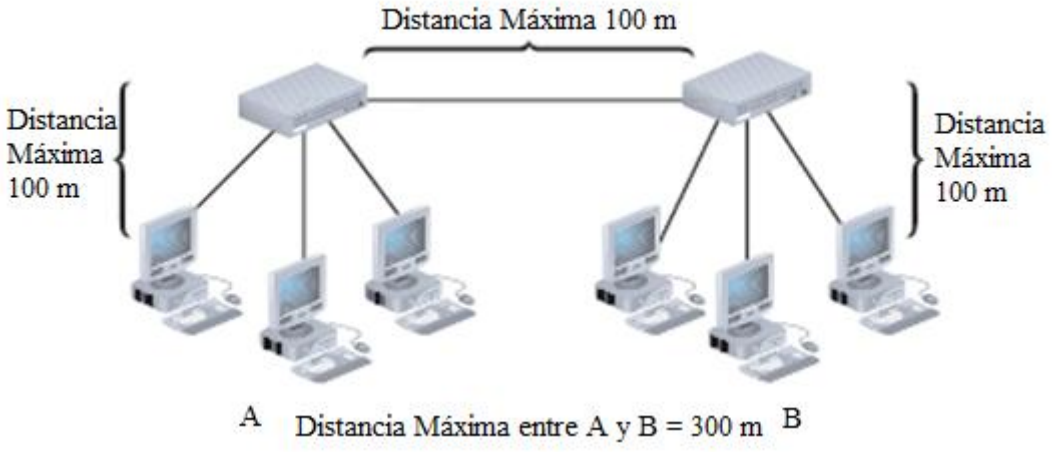


**Figura 2-15**. ***Red 100Base-T***

**Fuente: Dean, 2009**

**100Base-FX**. El estándar 100Base-FX especifica que una red es capaz de transportar datos a una velocidad de 100-Mbps utilizando la transmisión de banda base y cableado de fibra óptica. 100Base-FX requiere fibra multimodo que contiene al menos dos filamentos de fibra. En el modo semidúplex, una hebra se utiliza para la transmisión de datos, mientras que la otra hebra se utiliza para la recepción. En implementaciones full-duplex, ambos caminos se utilizan para el envío y recepción de datos.

100Base-FX tiene una longitud máxima de segmento de 412 metros si se utiliza transmisión semi-duplex y 2000 metros si se utiliza full-duplex. El estándar permite máximo un repetidor para conectar los segmentos.

Éste estándar, como 100Base-T, también se considera Fast Ethernet y se describe en el estándar 802.3u del IEEE. Las empresas en sus redes de comunicación de fibra pueden combinar 100Base-TX y 100Base-FX dentro de una misma red. Para ello, transmisores, receptores en los ordenadores y dispositivos de conectividad deben tener tanto RJ-45 como puertos SC, ST, LC o MT-RJ para fibra. Alternativamente, un convertidor de medios 100Base-TX a 100Base-FX, puede ser utilizado en cualquier punto en la red para interconectar los diferentes medios de comunicación y convertir las señales de un estándar a las señales que trabajan con la otra norma.

Existen otros estándares como 1000Base-LX, 1000Base-SX y otros, los cuales no se expondrán en detalle, pero se expresan a continuación en la siguiente tabla.

**Tabla 2-5.** ***Estándares Ethernet***

| Estándar | Máxima velocidad de Transmisión (Mbps) | Máxima distancia por segmento (m) | Medio Físico |
|---|---|---|---|
| **10Base-T** | 10 | 100 | UTP Cat 3 o superior |
| **100Base-TX** | 100 | 100 | UTP Cat 5 o superior |
| **1000Base-T** | 1000 | 100 | UTP Cat 5 o superior (preferiblemente Cat 5e ) |
| **10GBase-T** | 10.000 | 100 | Cat 6 o Cat 7 preferiblemente |
| **100Base-FX** | 100 | 2000 | MMF |
| **1000Base-LX** | 1000 | Hasta 550<br>5000 | MMF<br>SMF |
| **100Base-SX** | 1000 | Hasta 500 | MMF |
| **10GBase-SR y 10GBase-SW** | 10.000 | Hasta 300 | MMF |
| **10GBase-LR y 10GBase-LW** | 10.000 | 10.000 | SMF |
| **10GBase-ER y 10GBase-EW** | 10.000 | 40.000 | SMF |

### Cable UTP

El cable UTP (unshielded twisted pair) o par trenzado sin blindaje, consiste en uno o más pares de hilos de cobre aislados provistos de un revestimiento de plástico. Como su nombre implica, el UTP no contiene blindaje adicional para los pares trenzados. Como resultado es menos costoso y menos resistente al ruido que STP (shielded twisted pair). [36]

TIA / EIA es el consorcio que designa estándares para el cableado de par trenzado. Para manipular el cableado de una red, es necesario estar familiarizado con las normas para su uso en redes modernas, en particular CAT 3 y CAT 5 o superior:

- **Cat 3** (Categoría 3) es una forma de UTP que contiene cuatro pares de hilos y puede transportar hasta 10 Mbps de datos, con un posible ancho de banda de 16 MHz Cat 3 ha sido tradicionalmente utilizado para 10-Mbps con protocolo Ethernet.

- **Cat 4** (Categoría 4) es una forma de UTP que contiene cuatro pares de hilos y puede soportar una tasa de transmisión hasta 16 Mbps. No es común en las nuevas redes y se utilizaba antiguamente en redes token ring de 16 Mbps o en redes de 10 Mbps con protocolo Ethernet. Se garantiza para señales de hasta 20 MHz y ofrece más protección contra la interferencia y la atenuación que el Cat 3.

- **Cat 5** (Categoría 5) es una forma de UTP que contiene cuatro pares de hilos y admite una tasa de transmisión de hasta 1000 Mbps y permite un ancho de banda de 100 MHz.

- **Cat 5e** (Category 5 Mejorada) es una versión superior del cableado Cat 5 que contiene cobre de alta calidad, ofrece una relación de torsión alta y utiliza métodos avanzados para reducir la interferencia. La Cat 5e puede soportar un ancho de banda de hasta 350 MHz, tres veces más de la capacidad del Cat 5 ordinario.

- **Cat 6** (Categoría 6) es un cable de par trenzado que contiene cuatro pares de hilos de cobre, cada uno envuelto en un papel de aluminio de aislamiento. Otra lámina de aluminio sirve de aislamiento del conjunto de pares, y una envoltura de plástico resistente al fuego cubre la segunda capa. El aislamiento de papel de aluminio proporciona una excelente resistencia a la interferencia y permite a Cat 6 soportar una señal de 250 MHz con por lo menos seis veces más de rendimiento que el soportado por Cat5 regular.

- **Cat 6e** (Categoría 6 Mejorada) es una versión superior del cableado Cat 6 que reduce la atenuación y la interferencia, y permite aumentar los límites de longitud de segmento para el exceso de potencial de las redes tradicionales. El Cableado Cat

6e es capaz de un ancho de banda de 550 MHz y puede transmitir datos de forma confiable a varios Gbps.

- **Cat 7** (categoría 7) es un cable de par trenzado que contiene varios pares de cables, cada uno rodeado por su propia protección, luego se envuelven en una protección adicional debajo de la envoltura.

**Terminación de cable de par trenzado**

La terminación adecuada del cable es un requisito básico en los nodos de una red para poder comunicarse. Más allá de eso, las terminaciones deficientes pueden conducir a la pérdida de paquetes o interferencia y en consecuencia errores en la comunicación de la red. Entonces, seguir las Normas de terminación es fundamental. La TIA / EIA especifica dos métodos diferentes para la inserción de cables de par trenzado en conectores RJ-45: TIA / EIA 568A y TIA / EIA 568B.

Funcionalmente, no hay diferencia entre estos estándares, solo que es necesario asegurarse que se utiliza el mismo estándar en cada extremo de la conexión, de modo que los datos se transmitan y se reciban correctamente. En la figura 2-16 puede apreciarse la conexión tipo A y en la figura 2-17 se muestra la combinación de cables para una conexión tipo B. [37]


**Figura 2-16.** ***TIA/EIA 568A***

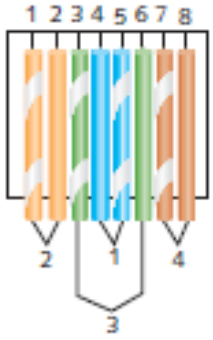


**Figura 2-17**. ***TIA/EIA 568B***

**Fuente: Dean, 2009**

**MMF (Fibra Multimodo)**

MMF (fibra multimodo) contiene un núcleo con un diámetro mayor que la fibra de monomodo (entre 50 y 115 micras de diámetro, mientas que el tamaño más común es 62,5 micras), sobre la cual pulsos de luz generados por un láser o LED viajan en diferentes ángulos. Se encuentra comúnmente en los cables que conectan un enrutador a un switch o un servidor en el *backbone* de una red.

La Figura 2-18 muestra una vista simplificada de cómo viajan las señales a través de fibra multimodo. Debido a su fiabilidad, la fibra se utiliza principalmente como un cable que conecta los segmentos de una red. [38]

El cable de fibra óptica ofrece las siguientes ventajas sobre cableado de cobre:

• Rendimiento extremadamente alto.

• Alta resistencia al ruido.

• Excelente seguridad.

• Capacidad para transportar señales a distancias mucho más largas antes de requerir repetidores.

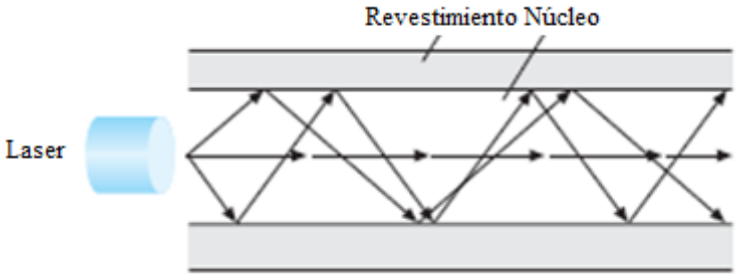


**Figura 2-18.** ***Fibra Multimodo***

**Fuente: Dean, 2009**

# CAPITULO III

## LEVANTAMIENTO DE INFORMACIÓN

### 3.1 Evaluación de las necesidades

En esta fase se visitó cada una de las sedes de la empresa, las cuales conformaran la red WAN, con el fin de evaluar sus necesidades en cuanto a ancho de banda requerido para el intercambio de datos con el nodo central y los equipos mínimos necesarios para la existencia de una red LAN en cada sede.

Se tomo en cuenta para el levantamiento de información: cantidad de equipos y usuarios, acceso inalámbrico, servicios y equipos necesarios para la red. Para estimar la cantidad de usuarios para VoIP que existirán en cada sede, se considero tanto las divisiones físicas de las oficinas, como los departamentos que allí funcionan.

El ***levantamiento de información*** se expresa en forma detallada para cada una de las sedes, a continuación.

#### 3.1.1 Artigas

Esta sede cuenta con dos pisos administrativos y un taller, en total se utilizan 10 computadoras de escritorio y 2 impresoras, el servicio de internet se obtiene a través de un modem ADSL de CANTV con una velocidad de 2048 Kbps. Los servicios de esta red son administrados mediante un Enrutador con acceso inalámbrico y un Switch de 8 puertos.

La planta baja posee 5 estaciones de trabajo de las cuales 2 están cableadas hacia el Switch y las otras 3 se conectan en forma inalámbrica con el Enrutador que administra la red. A disposición de los usuarios existe una impresora que se encuentra compartida mediante configuración local en una de las estaciones.

Los equipos de la planta baja, que se conectan de forma inalámbrica suelen tener conflictos para establecer conexión con la red, esto puede ser debido a que el Enrutador se encuentra en el piso superior y hay obstáculos como pisos, paredes, etc., que pueden provocar la atenuación de la señal y la pérdida de datos.

El piso superior tiene 4 puestos de trabajo de los cuales 2 se encuentran cableados y los otros 2 se conectan de forma inalámbrica. La impresora se encuentra conectada a una estación, a diferencia de la planta baja la impresora no está compartida por lo que si una de las estaciones necesita imprimir no lo puede hacer en red. El punto de acceso ubicado en el taller se encuentra aproximadamente a una distancia de 40 m (recorrido de cableado) desde el Switch. Esta locación posee 1 sola estación de trabajo y se conecta por medio de cable UTP, además no posee impresora.

El hecho que las impresoras estén conectadas de manera local a una de las estaciones de trabajo y éstas mediante configuración local sean compartidas, permite utilizar las impresoras desde todas las estaciones. Una desventaja de este tipo de configuración es que si la estación de trabajo donde se encuentra la impresora no está encendida, no será posible imprimir desde ninguna de los puestos de trabajo.

### 3.1.2 La Yaguara

Esta sucursal se encuentra en remodelación, por lo que el levantamiento de la información es una proyección de la cantidad de estaciones de trabajos que se van a instalar.

La sede está conformada por dos inmuebles y en total estará comprendida por 20 PCs y 2 impresoras, el servicio de internet es prestado por la empresa CANTV a través de un modem ADSL y ofrece una velocidad de 2048 Kbps. La red existente posee solo un Enrutador con acceso inalámbrico que se encarga de distribuir y administrar los servicios.

La estructura ya construida tiene 4 equipos de escritorio (PC), de los cuales 2 están conectados mediante cable UTP y dos de forma inalámbrica con el Enrutador, además hay una impresora que está conectada a una de las estaciones de trabajo y se encuentra configurada para ser compartida con los otros equipos.

El inmueble en construcción se localiza a unos 60 m aproximadamente, de la estructura existente, y su red estará conformada por 17 estaciones terminales de las cuales 2 son Laptops, 14 equipos de escritorio y una impresora.

### 3.1.3 Zona Rental

La red en esta sede cuenta con un total de 23 equipos y 1 impresora, distribuidos en dos oficinas. El servicio de internet se obtiene de la empresa de servicios (CANTV), pero es suministrado y administrado por la Alcaldía de Caracas que opera la red del edificio.

La administración de la red local en la oficina de SUPRA se hace a través de un Enrutador con acceso inalámbrico y un Switch no administrable de 24 puertos que se encuentran en la oficina principal, el Switch se comunica a través de un cable UTP con otro de 16 puertos ubicado en otra oficina que reparte el servicio a 8 PCs.

En la oficina principal operan 12 PCs de escritorio que están cableadas hasta el Switch, y 3 laptops que acceden a la red de forma inalámbrica. En esta oficina se

encuentra la impresora que está conectada mediante cable UTP a la red, por lo que todos los equipos conectados a la misma pueden imprimir de manera remota.

En la segunda oficina hay 8 puestos de trabajo, todas las maquinas están conectadas físicamente mediante un cable UTP a un Switch de 16 puertos que distribuye el servicio. En esta oficina no se encuentra físicamente ninguna impresora.

### 3.1.4 Las Mayas (Nodo central)

#### 3.1.4.1 Funcionamiento de la Red Original

En las Mayas está ubicada la sede principal, en ella hay un total de 65 PC, 10 servidores, 10 laptops y 4 impresoras. El servicio de internet que proporciona CANTV a esta sede es ABA de 2048 Kbps.

La sucursal está conformada por 4 edificaciones separadas de la siguiente manera: un edificio administrativo, una estructura que funciona como peso para los camiones llamado ´´La Romana´´, un local que funciona como sala de control y un edificio de Seguridad integral, todas deben formar parte de la red.

La red LAN en el edificio administrativo funciona casi en su totalidad de manera inalámbrica, un Enrutador inalámbrico central administra la red.

La conexión desde el modem hasta el armario (FXB) donde se encuentran los pares trenzados que dan el servicio ADSL de CANTV, se realiza mediante un cable UTP, del cual sólo se utiliza 1 par trenzado, para la conexión de la línea telefónica, este recorrido es de aproximadamente 120 m.

Desde el centro de datos, donde se alojan los servidores y se distribuyen todos los servicios, hasta el modem que da el servicio de internet (***La Romana***), la

conexión se hace a través de un arreglo de ***backbone serial***, cuyo medio físico es cableado UTP con una extensión de aproximadamente 220 m, la señal logra llegar gracias a 4 Switches que regeneran la señal hasta el centro de datos. Este recorrido tiene varios saltos, debido al arreglo utilizado, lo que ocasionan pérdida de paquetes y un servicio deficiente de Internet.

Este enlace, adicionalmente da acceso a los usuarios que se encuentran en ***La Romana*** (punto donde se encuentre el modem) y a otro segmento de red que alberga un servidor que se encuentra en el centro de datos

La conexión de La Romana llega a un Switch capa 2 en el centro datos, este Switch se conecta con el segmento de la red que aloja el servidor de una aplicación que usa La Romana y a su vez se conecta con el Enrutador central ubicado en el área de oficinas. La conexión regresa desde el Enrutador al centro de datos, a dos Switch capa 2 conectados en cascada que se encargan de repartir el servicio de red a las computadoras que no acceden a la misma mediante el enrutador inalámbrico, si no que se encuentran físicamente conectadas a los Switches. En la *Figura 3-1*, se muestra un diagrama de las conexiones mencionadas anteriormente.

El Enrutador inalámbrico ofrece el servicio DHCP, el control de acceso a servidores web, se hace a través de un servicio libre llamado ``Open dns´´, en el cual se bloquean las paginas no laborales mediante configuración local, sin necesidad de tener un servidor que se encargue del filtrado web. La desventaja de este servicio es que un usuario con cierto conocimiento en informática, podría cambiar directamente en su equipo la configuración y no pasar por el filtro.

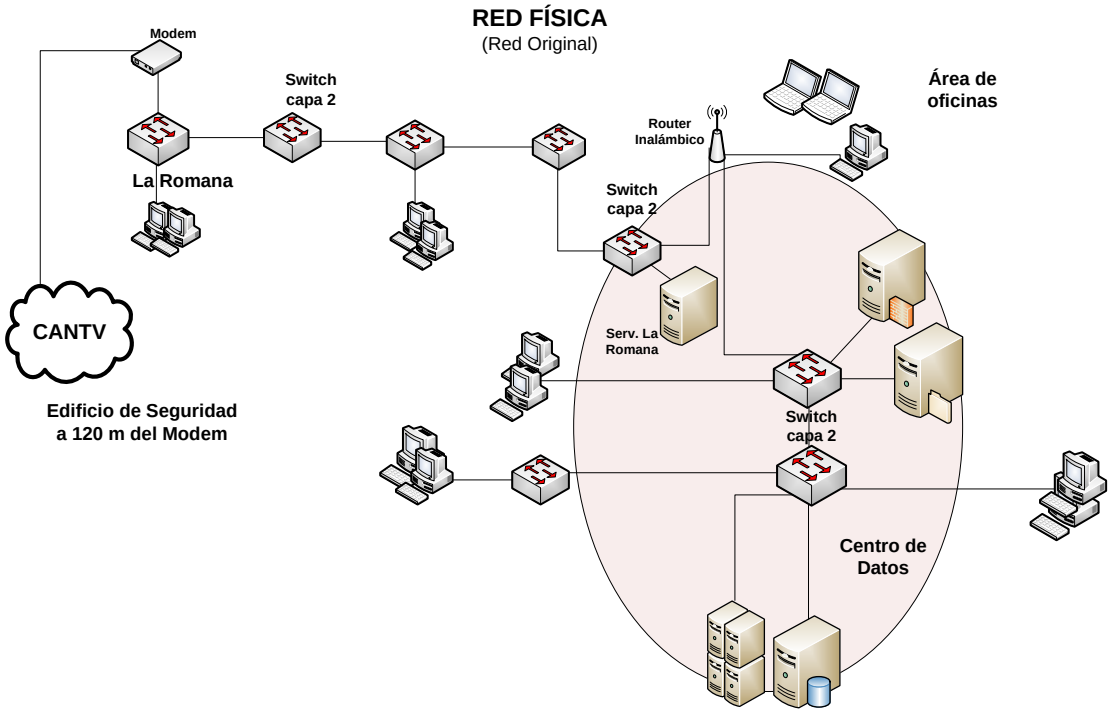


**Figura 3-1.** ***Red Física original***

Actualmente el edificio de Seguridad integral y taller no están conectados a la red, pero tienen acceso a internet mediante otro servicio ABA de CANTV con una velocidad de 1024 Kbps. El servicio es intermitente por problemas con el cableado de planta externa por parte de la empresa que presta el servicio (CANTV), por lo que los usuarios la mayoría del tiempo no tienen acceso a internet. Sala de control no tiene acceso ni a la red local ni a internet.

### 3.1.4.2 Descripción de la distribución de las estructuras

A fin de conocer las necesidades de la empresa en cuanto a conexión física, se realizaron mediciones de longitud entre los espacios físicos de la misma utilizando un dispositivo llamado odómetro.

Las conexiones entre los edificios tienen las siguientes características:

- *Distancia entre seguridad integral y taller* :
  HAY UNA DISTANCIA DE **100 m**
  Este tramo tiene instalado fibra con convertidores fibra-Ethernet en sus extremos. Este tramo no se encuentra operativo.
- *Distancia entre taller y La Romana* :
  HAY UNA DISTANCIA DE **20 m**
  Este tramo tiene una tubería por donde viaja el cable UTP y actualmente no está operativo.
- *Distancia entre La Romana y sede administrativa (centro de datos)*:
  HAY UNA DISTANCIA DE **220 m**
  Este tramo tiene tubería para cableado UTP. Actualmente solo existe una conexión operativa con cable UTP para la comunicación con el servidor, 4 switches se encuentran en el camino de La Romana hasta el centro de datos.
- Distancia entre taller y sala de control
  HAY UNA DISTANCIA DE **15 m**
  Este tramo no está construido, no tiene tuberías ni ninguna estructura por donde pueda viajar el cableado y seria una derivación del taller hacia sala de control.

Cabe destacar que las distancias fueron medidas en línea recta entre las estructuras, y no necesariamente éste será el recorrido del cableado, por lo cual la distancia puede aumentar en algunos metros. A continuación se presenta un diagrama de la distribución de los edificios descrita anteriormente.

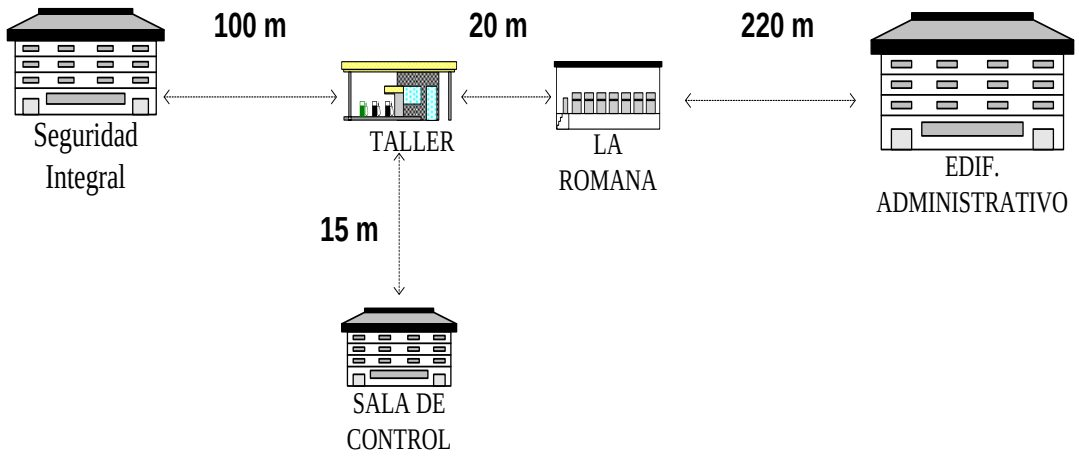


**Figura 3-2.** ***Distribución física de los edificios en Las Mayas***

### 3.1.5 Totalización de datos

Los datos recolectados en el levantamiento de información se presentan en una tabla que contiene el total de equipos, cantidad potencial de usuarios VoIP y las condiciones existentes relevantes para la interconexión de las sedes a través de la red WAN.

**Tabla 3-1.** ***Totalización de datos***

| SEDE | ESTACIONES TERMINALES | USUARIOS VoIP | FxB |
|---|---|---|---|
| **Artigas** | 10 PC<br>2 impresoras | 3 | NO HAY,<br>DIRECTO DE LA MANGA |
| **La Yaguara** | 20 PC<br>2 LAPTOPS<br>2 impresora | 3 | NO HAY, DIRECTO DE LA MANGA |
| **Zona Rental** | 26 PC<br>3 LAPTOPS<br>1 impresora | 9 | SI HAY,<br>PERO NO EXISTEN LINEAS DISPONIBLES |
| **Las Mayas** | 65 PC<br>10 LAPTOPS<br>4 impresoras<br>10 servidores | 9 | SI HAY,<br>Y EXISTEN LINEAS DISPONIBLES |

**NOTA**: Para optimizar el uso de recursos no se consideró la cantidad usuarios para VoIP en base a número de usuarios, sino que se tomo en cuenta tanto las separaciones físicas entre los equipos, como los departamentos para los cuales los mismos operan. Cabe destacar que las variables que atañen el servicio de VoIP, superan el alcance de este proyecto.

# CAPITULO IV

## DISEÑO Y PROPUESTA DE LAS REDES

### 4.1 Red WAN

La propuesta de una red WAN se genera como respuesta a la necesidad de la empresa SUPRA-Caracas de intercambiar datos entre sus sedes. De esta manera será posible centralizar y disponer de la información para automatizar procesos como: nómina, control operativo, compras, pagos, inventarios, etc. Se podrán ofrecer servicios de voz y correo electrónico así como el monitoreo operativo de toda la red, además se logrará dar asistencia remota a los usuarios, haciendo más eficiente el servicio para los mismos.

#### 4.1.1 Topología lógica

En la sección de topología lógica se expondrán tanto el tipo de topología, como los servicios y configuraciones que se proponen implementar en la red, además se hará referencia a los equipos con los que debe contar la red para lograr dichas propuestas.

**Selección de topología**

Para la interconexión entre las sedes se propone una topología tipo estrella. Este tipo de topología tiene facilidad de escalamiento, cualquier nueva sede que se adjunte a la empresa sólo requerirá de una interconexión con el nodo central de la red, y así podrá disponer y disfrutar de los servicios que ésta ofrezca. Otra ventaja de esta

topología es que la falla de cualquier dispositivo de conexión o nodo no afectará el funcionamiento de toda la red, sino que sólo afectará la red LAN asociada al nodo con dicha falla.

Como este tipo de topología incluye un punto de conexión centralizado, se puede mover fácilmente, debido a esto y a su tolerancia a fallas, la topología en estrella se ha convertido en el diseño más popular utilizado. Redes individuales que utilizan esta topología, están comúnmente interconectadas con otras a través de Switches o Enrutador para formar topologías más complejas. La mayoría de las redes Ethernet se basan en la topología en estrella.

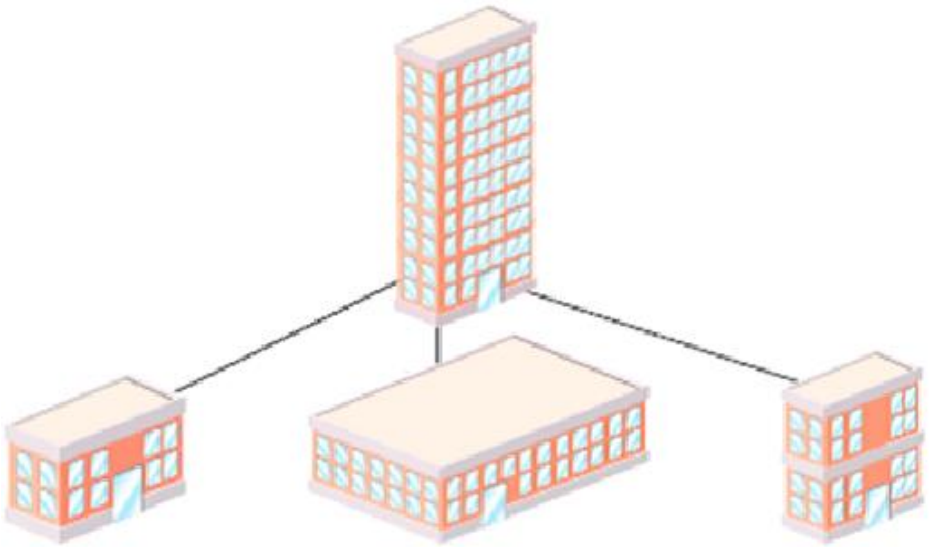

**Figura 4-1**. ***Red WAN con Topología estrella***

**Fuente: Dean (2009)**

### Nodo Central

El nodo central estará ubicado en la sede Las Mayas, desde el cual se pueda administrar toda la red. La elección de esta sede como nodo central se debe a que la mayor cantidad del personal administrativo de la empresa opera en esta localidad, en

consecuencia el grueso de los procesos se desarrollan en la misma: pagos, compras, despachos de camiones, control de operaciones, etc. Además, esta sede cuenta con el espacio físico para la instalación del centro de datos de la red.

**Aplicaciones y Servicios**

Se propone instalar ciertos equipos que permitan que la red opere de forma segura y eficiente. Para ello es indispensable la implementación de un **Firewall.** Este equipo permite proteger a la red de ataques externos, accesos indeseados, virus, etc., además de otras ventajas.

También será necesario un servidor de correo electrónico para que los usuarios de la red no dependan de un servidor externo para este servicio, un servidor DHCP que pueda *entregar* direcciones IP validas a los usuarios, así como un DNS, adicionalmente se tendrá que considerar un servidor para VoIP si se desea ofrecer este servicio.

Todos los servidores ya existentes o en desarrollo estarán alojados en el nodo central, estos son: servidor de aplicación de cálculo de nómina, DHCP, DNS, servidor de aplicaciones de actividades operativas, de respaldo, servidor web, de correo, de VoIP, de recaudación y servidor de La Romana.

Las aplicaciones deben ser accesibles desde cualquier sede. El servidor web y el de correo deben tener acceso a través de internet, por lo que para estos dos servicios es necesario una red aislada a la cual se puede acceder desde el Firewall, pero que a su vez éste pueda evitar el acceso, de un usuario no autorizado, hacia la LAN de cualquiera de las sedes. La solución para este planteamiento es una **DMZ**, ésta permite aislar los servicios públicos a los usuarios y proteger a la red privada.

En el Firewall además es posible crear listas de acceso (***ACL***). Estas listas nos permitirán seleccionar qué VLAN o usuario específico, tiene acceso a determinado servicio, lo que es necesario ya que la red posee usuarios que deben tener acceso a servidores de distintas VLAN. *Estas VLAN se verán en forma más amplia posteriormente*.

A fin de tener un manejo más eficiente del ancho de banda se propone un servidor de caché en cada nodo de la red WAN, de manera tal que se puedan almacenar localmente objetos y archivos temporales de las páginas más concurridas en cada sede, y así no gastar recursos de la red en descargas de objetos que se utilizan con frecuencia.

**Enlaces y rutas**

Para la conexión entre el nodo central y las demás sedes, se plantean servicios de ***VPN*** Ethernet en capa 2. En esta arquitectura, los enlaces son una especie de ***tuberías virtuales*** que interconectarán las sedes. Este tipo de conexión tiene lugar en la red pública de transporte de datos de CANTV, pero al mismo tiempo se encuentra aislada del tráfico de la misma. Esto es posible gracias a que VPN encapsula protocolos de capas superiores, en un proceso conocido como efecto túnel o en ingles ***tunneling***, garantizando así la interoperabilidad y seguridad sin importar el tipo de conexión que se utilice para lograr el enlace. VPN en capa 2, permite manejar las direcciones IP como si estuvieran en una red de área local.

En el caso de nuestra red serán necesarios enlaces punto-multipunto, entre cada una de las sedes y el nodo central, y un enlace punto a punto que será para el acceso a internet en el nodo central de la WAN.

Para el acceso a internet se tendrán una o varias direcciones IP públicas fijas para la empresa, es por esto que se hace necesario configurar en el Enrutador un

mecanismo de traducción de IP para que las direcciones privadas de la red tengan acceso a internet. Este mecanismo es denominado NAT, el cual se encarga de traducir direcciones IP privadas, al rango de las direcciones públicas.

En la siguiente figura se muestra un diagrama que muestra la topología para la red WAN.

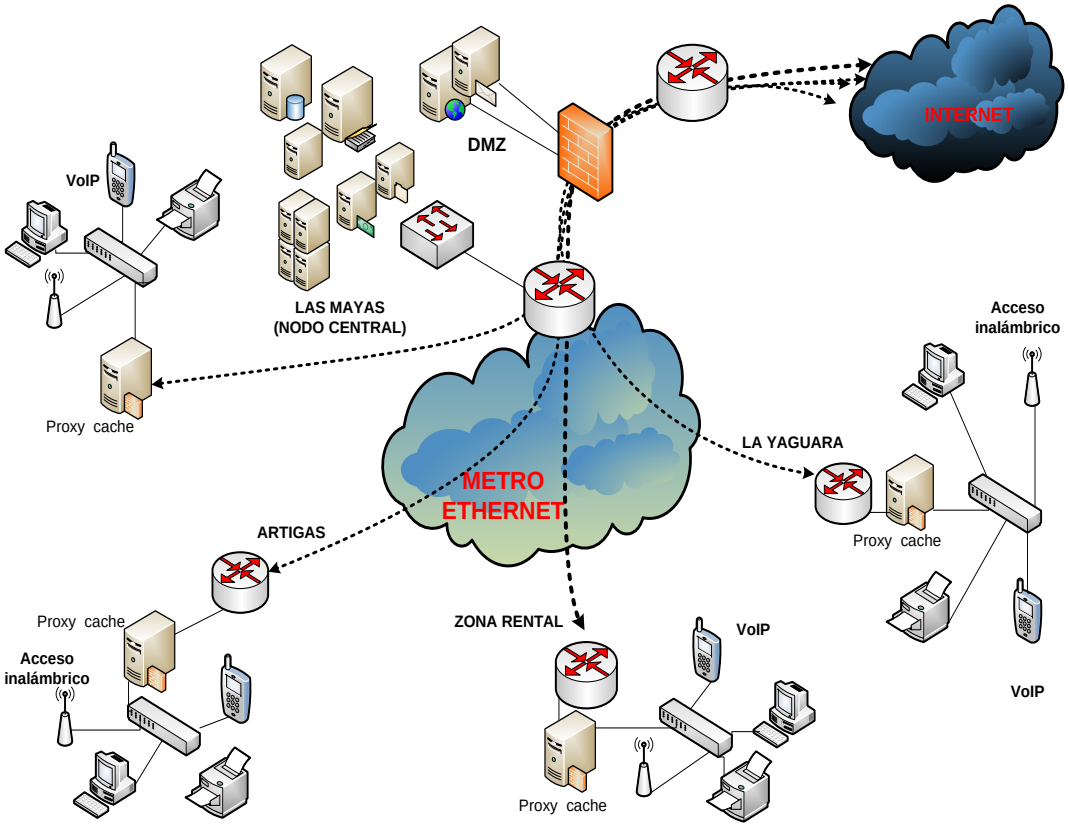


**Figura 4-2.** ***Topología lógica WAN***

La estructura de la red puede verse como un diseño jerárquico, donde el núcleo es el firewall y los Enrutadores contiguos a él, la capa de distribución la conforman los Enrutadores de cada una de las sedes, y por último la capa de acceso que estaría conformada por los switches y equipos terminales de las LAN.

### 4.1.2 Topología física

La configuración física de la red se podría calificar como punto-punto desde el enrutador de cada sede hacia la red de CANTV, ya que la parte que concierne el backbone de CANTV es virtualmente invisible en lo que respecta a conexiones físicas. Aun así, si se considera el backbone como una serie de Switches interconectados, se obtiene la topología en anillo.

En el siguiente diagrama se muestra la topología física de la WAN.

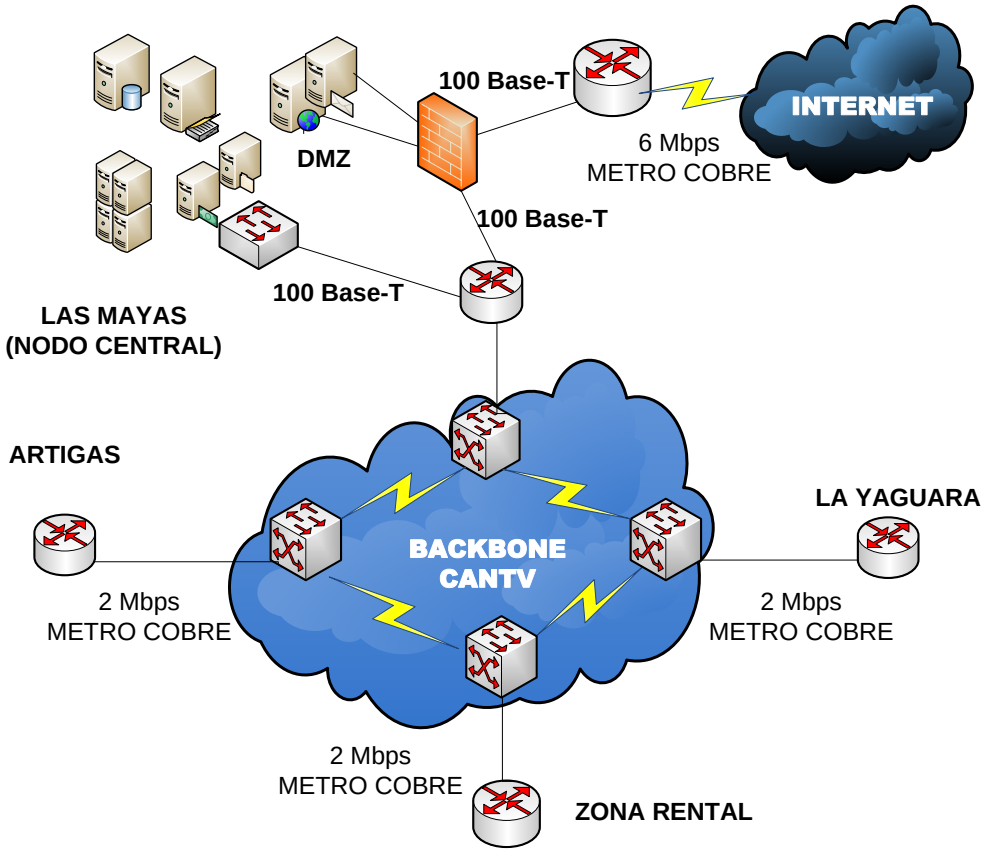


**Figura 4-3.** ***Topología física WAN***

La conexión entre los Enrutadores de cada una de las sedes y el backbone de CANTV es a través de pares de cobre, utilizando protocolos Ethernet.

En el nodo central las conexiones entre el Enrutador, el Firewall, los Switches y los servidores, se realiza con cable UTP, cat 5e o superior, utilizando el protocolo 100 Base-T (*fastEthernet*), y por último el Enrutador que da acceso a internet tiene conexión con la plataforma de CANTV a través de múltiples pares de cobre utilizando protocolo Ethernet.

## 4.2 Propuestas para redes de área local (LAN) de las sedes

En esta sección se exponen propuestas para cada una de las redes locales pertenecientes a las sedes, es importante destacar que sólo se explicará en detalle el diseño de la red LAN para el nodo central (Las Mayas).

#### 4.2.1.1 Artigas

Se propone instalar y configurar una red que abarque los 12 equipos terminales (*PC e impresoras*), de manera que los usuarios puedan compartir los recursos entre sí. Son necesarios un Enrutador y un Switch de mínimo 16 puertos, de esta manera todos los equipos podrán estar conectados físicamente a la red.

Ya que las dimensiones de la locación lo hacen posible, se plantea cablear cada uno de los puestos de trabajo, de esta manera se garantiza un servicio más confiable. Todos los dispositivos centrales se pueden resguardar en un Rack de pared ubicado en el segundo piso y de ahí distribuir el cableado a los equipos terminales.

Las impresoras se conectarán directamente a la red mediante un puerto tipo RJ-45 utilizando protocolo Ethernet, lo que permite que éstas sean independientes del estado (encendido o apagado) de las estaciones de trabajo para imprimir. Esta

configuración permitirá administrar mejor los recursos de dicha red. ***Es necesario un Enrutador con capacidad para la conexión con la red WAN.***

#### 4.2.1.2 La Yaguara

Para la implementación de la red en esta sede, son necesarios un Enrutador y un Switch de 24 puertos, de manera que sea posible interconectar los 20 equipos a través de una red física.

En el inmueble que se va a construir existe el espacio ideal para la instalación de un rack que resguarde los equipos de la red. En este sitio es posible alojar los equipos que se encargarán de la distribución de los servicios y de la interconexión con la red WAN.

Desde este punto se debe interconectar ambas edificaciones mediante cable UTP Cat 5e. Este cableado UTP cumple con el estándar 100Base-T, ya que la distancia no supera los 100 m. El cableado debe llegar a un Switch simple de 8 puertos en la estructura ya construida, el cual se encargará de distribuir el servicio tanto a los equipos de escritorio como a las impresoras en esa edificación.

Las impresoras estarán conectadas directamente a la red de manera que la impresión no dependa de si el equipo de escritorio está encendido o no. Adicionalmente se debe instalar un punto de acceso inalámbrico, el cual puede ser un Enrutador configurado como tal, de forma que se les pueda dar el servicio a los dispositivos inalámbricos. ***Es necesario un Enrutador con capacidad para la conexión con la red WAN.***

#### 4.2.1.3 Zona Rental

Se recomienda la instalación de una nueva impresora a la red, para que los usuarios de la oficina secundaria tengan a su disposición una impresora ubicada físicamente en su área de trabajo.

Debido a que el servicio de internet es prestado por la alcaldía, no es posible administrar de manera eficiente el ancho de banda, además de controlar el acceso a las direcciones que el administrador de dicha red desee. Se plantea implementar un servicio independiente para administrar mejor los recursos de la red.

Es recomendable cambiar el Switch no administrable por uno que si lo sea, de esta manera se podrán crear VLANs para un mejor desempeño de la red. ***Es necesario un Enrutador con capacidad para la conexión con la red WAN.***

#### 4.2.1.4 Las Mayas (Nodo Central)

Esta red ya existía, constaba con cableado UTP que recorría largas distancia desde el acceso a internet hasta los usuarios, lo que tenía como consecuencia una pérdida de datos debido a la atenuación de la señal. Además se emplean varios switches intermedios colocados en el camino para regenerar dicha señal, lo que genera mayor cantidad de saltos y difusión (broadcast) innecesaria. Se hizo un replanteamiento de esta red para utilizar los recursos ya existentes y optimizar los servicios.

En general, se plantea la unificación de todos los edificios que conforman la sede, en una red de datos capaz de interconectar cada área de trabajo, y de esta forma ofrecer los servicios disponibles en la red. El desarrollo de esta propuesta se expondrá posteriormente, de manera detallada en cuanto a topología lógica y física.

#### 4.2.1.4.1 Topología Lógica

**Selección de la topología**

Para la red LAN se propone una topología lógica en ***estrella***, anteriormente se han mencionado algunos beneficios de esta configuración. Es importante resaltar que la comunicación en la red será en su mayoría con servicios centralizados, por lo que esta topología es la indicada de acuerdo a las necesidades de la empresa.

En los próximos párrafos se expondrán los servicios y la forma de comunicación que fueron pensados para la red LAN del nodo central. Este diseño se hizo según las necesidades de dicha sede y de la empresa en general, ya analizadas en el capítulo de levantamiento de información. En él se cumplen y respetan las normas contempladas en los estándares Ethernet.

**Redes virtuales (VLAN)**

Para una mejor desempeño de la red se plantea la creación de VLANs (estándar IEEE 802.1q), con lo que se conseguirá agrupar equipos terminales que están separados físicamente, en redes virtuales afines que puedan disfrutar de opciones especiales de seguridad y servicios.

Las VLANs permiten crear dominios de difusión o *broadcast*, los dominios de *broadcast* ayudan a que la red no se sature con las peticiones de todos los usuarios, si no que en su lugar las peticiones sólo se limitan a su dominio, optimizando así el uso de los recursos de la red.

Dichas VLANs pueden aplicar para todas las LAN en las sedes de la empresa, lo que permitirá a través de la WAN, que los usuarios pertenecientes a la misma VLAN tengan los servicios y las protecciones determinadas para ésta.

Debido a que en la empresa se desarrollan procesos que son independientes unos de otros y existen algunos de estos que necesitan protección especial como lo son: Control de nómina y La Romana, la implementación de este tipo de configuración resulta muy favorable, de esta manera se aislarían dichos procesos y el desempeño de la red mejoraría considerablemente, además de incrementar la seguridad de los mismos.

Conjuntamente con su mejora en el uso del ancho de banda las VLAN se valoran por su flexibilidad. Ellas pueden incluir puertos en más de un Switch. Además cualquier tipo de nodo puede pertenecer a una o más VLAN. Las VLAN se pueden vincular a los usuarios geográficamente distantes a través de una WAN, y pueden crear así pequeños grupos de trabajo dentro de las LAN.

Para los servicios de impresión se propone instalar al menos una impresora por VLAN, de esta manera no es necesario un servidor de impresión. La VLAN de internet se excluye de este planteamiento.

**Servidor Proxy-Caché**

Con la finalidad de optimizar el uso del ancho de banda, se propone la implementación de un servidor que almacene las peticiones frecuentes a internet, y así el desempeño de la red será mucho más eficiente. La razón de implementar un Proxy Caché, se enfoca en las repetidas peticiones a buscadores y páginas de interés laboral como el seguro social, páginas estatales y otras, a las que acceden los usuarios de la red de la empresa.

Para optimizar su eficiencia es importante que exista un proceso de mejora continua, de modo que se aproveche la información que proporcionan los registros producidos por el servidor, ajustando la configuración del proxy a los requisitos de nuestra organización. Es importante establecer al servidor como un Proxy transparente, de manera que los usuarios no noten el uso del mismo, además de esta forma no es necesario configurar el Proxy en los equipos terminales.

**Servidor de correo**

La instalación de un servidor de correo electrónico además de disminuir el tráfico que puedan generar el envío y recepción de correos de servidores externos, tiene ventajas adicionales como:

- Creación ilimitada de cuentas de correo electrónico.
- La cantidad de espacio para cada buzón es configurable (Cuotas).
- Podrá enviar correo a través de su servidor desde cualquier parte del mundo, a través de la Internet.

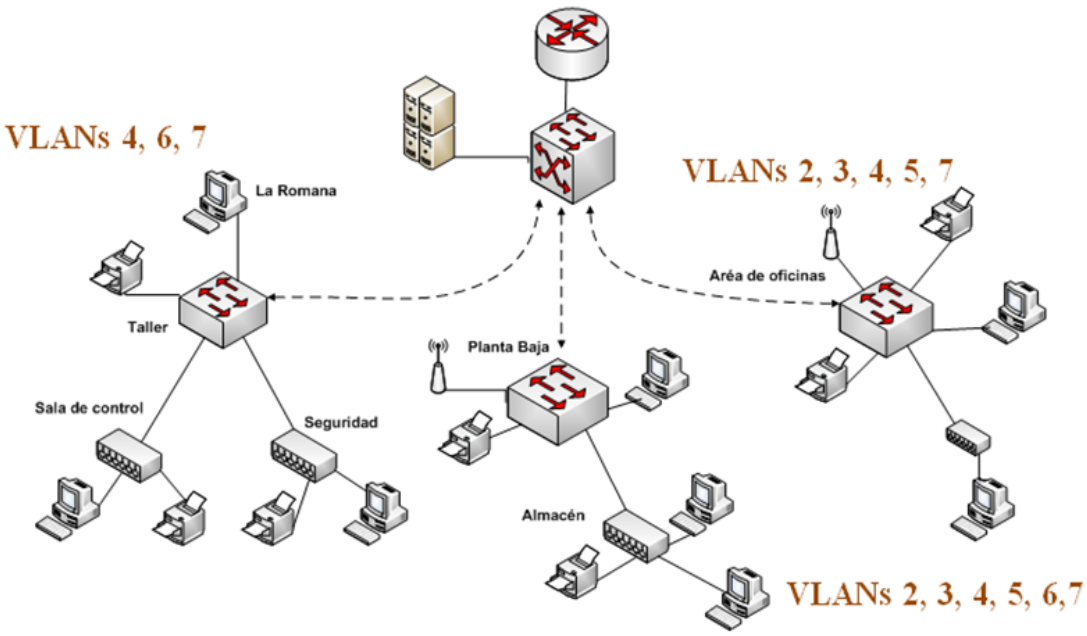


**Figura 4-4.** ***Topología lógica de la LAN***

Teniendo en cuenta todas las propuestas formuladas en esta sección para la LAN se muestra en siguiente figura un diagrama lógico de la misma

La selección de un Switch capa 3 en el núcleo, es debido a que esta clase de dispositivos tiene la posibilidad de ejecutar procesos de enrutamiento, lo que disminuirá el trabajo que tenga que desempeñar el Enrutador de borde. Además, la transferencia de paquetes puede ejecutarse de forma más directa, ya que no todos los paquetes tienen que viajar hasta el Enrutador. Por ejemplo, la comunicación entre VLANs podría llevarse a cabo en el Switch capa 3 sin necesidad de tener que hacer uso del enrutador.

Esta es una topología jerárquica, hecho que puede apreciarse con mayor claridad en la siguiente figura. El círculo ***rojo*** delimita lo que sería el ***núcleo*** de la red, también conocido como el *backbone* de alta velocidad de la red, siendo esencial para la interconexión entre los dispositivos de la capa de distribución

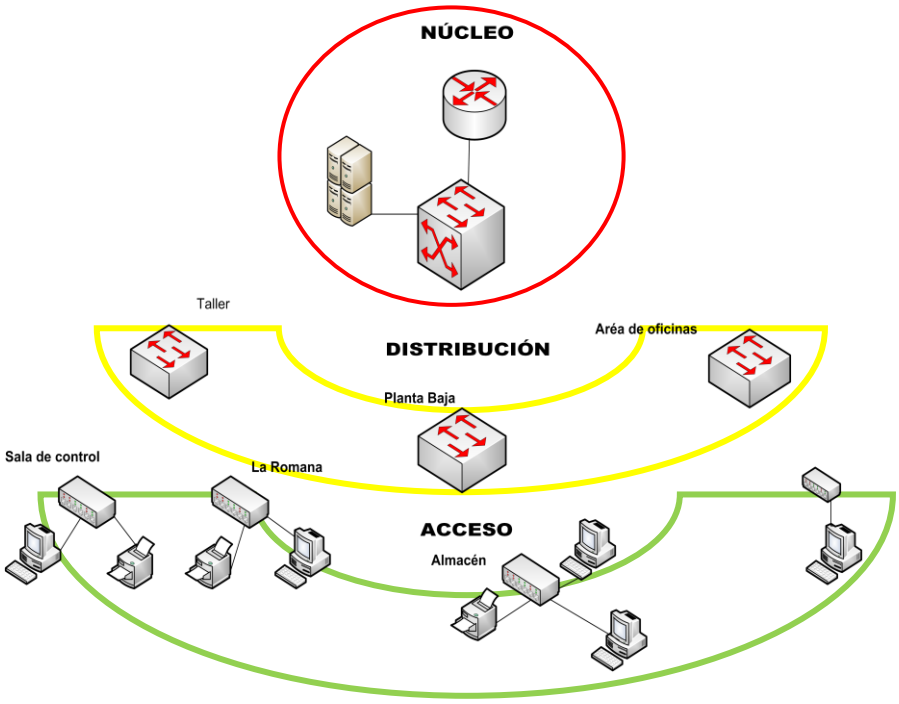


**Figura 4-5.** ***Red jerárquica***

La zona de color ***amarillo*** sería la capa de ***distribución*** que controla el tráfico de la red con dominios y políticas de *broadcast* para las VLAN y por último la zona ***verde*** sería la capa de ***acceso*** de una red con jerarquías, la cual comprende las interfaces que conecta a los equipos terminales de los usuarios.

#### 4.2.1.4.2 Topología Física

**Selección de topología**

Para la red LAN se propone una topología híbrida interconectada en una configuración ***Backbone distribuido.*** Esta red jerárquica permitirá conectar los puestos de trabajo a dispositivos más cercanos a ellos y así evitar que gran cantidad de cableado recorra largas distancias.

Esta topología se ajusta a la distribución física de nuestra localidad y a las necesidades de los usuarios. Además, permite un escalamiento sencillo y un gasto de capital limitado para el crecimiento de la red, debido a que más capas de dispositivos se pueden añadir a las capas existentes. Si la empresa contrata más personal, puede conectar otro Switch a uno de los existentes, y usar el nuevo para conectarlos a la red.

**Enlaces redundantes**

Se considera para la implementación física de la red, la utilización de enlaces redundantes, con esto la red será menos propensa a fallas. Este tipo de enlaces redundantes pueden producir *loops* o bucles de tráfico en la red, que generan errores en la conectividad ya que los paquetes tienen múltiples rutas para llegar a su destino, creando un ciclo infinito, ocasionando así la pérdida de los mismos y en consecuencia errores que no permiten el correcto funcionamiento de la red.

Otro error que se puede presentar, es la infinita generación de *broadcast* debido al bucle, lo que ocasionaría la saturación de toda la red. La implementación de enlaces redundantes sin la aparición de bucles de tráfico (*loops*), es posible gracias al protocolo STP. Este protocolo lo ejecutan la mayoría de los Switch por defecto, por lo que no necesita de una configuración especial. STP deshabilita virtualmente algunos de los puertos que completan un bucle. En el siguiente diagrama se presentan las interconexiones físicas entre los dispositivos de la red.

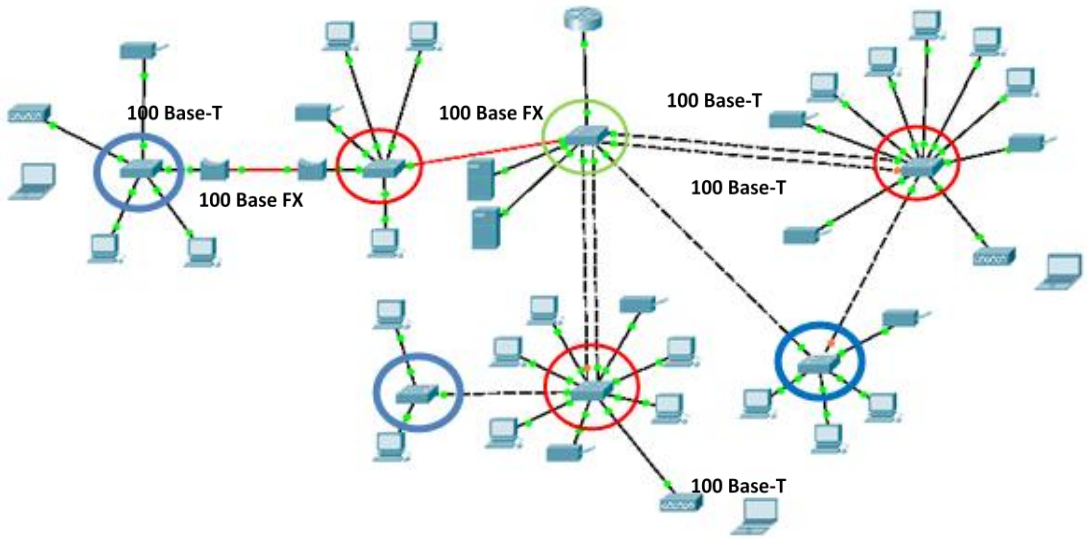


**Figura 4-6.** ***Topología Física LAN***

Las líneas punteadas representan cable UTP cruzado, esto quiere decir que los terminales de la conexión van invertidos, un extremo debe ser construido con la configuración A y el otro extremo con la configuración B para cables UTP. Este tipo de conexión se realiza entre dispositivos de la misma capa. Cabe destacar que actualmente la mayoría de los dispositivos reconocen cualquier combinación, directa o cruzada. Las líneas continuas son la representación de una conexión directa, puede ser A-A o B-B.

En el diagrama se puede notar que algunas conexiones tienen puntos rojos en las terminaciones de los enlaces, estos puntos rojos indican que el puerto se encuentra

deshabilitado de forma virtual ya que la conexión se cumple mediante otro cable. Estos son los cables redundantes que se proponen instalar, en caso de que uno falle estará el otro de respaldo.

Las líneas rojas representan los tramos de fibra óptica, en el tramo más a la izquierda de fibra, los equipos en los extremos del cableado son convertidores óptico/eléctrico Ethernet, dichos dispositivos ya se encuentran en el inventario de la empresa y por esta razón se utilizan en el diseño, en el otro tramo de fibra la conexión se hará a través de puertos de fibras en los Switches.

El tendido de fibra es necesario ya que la distancia es mayor a los 100 metros y basándonos en el estándar 100Base-T, la configuración de la red para esta distancia con cableado UTP, debe contar con máximo cuatro switches intermedios, pero originalmente existían cinco debido a la distancia y como se expuso anteriormente, esta configuración presentaba muchas fallas. Las fibras ópticas deben cumplir con el estándar 100Base-FX para fibra multimodo.

Los Switch con el círculo rojo, son Switches administrables, es decir, éstos permiten la creación y administración de VLANs. Los Switches en círculo azul son no administrables, lo que quiere decir que sólo reparten la misma VLAN en todos sus puertos. El switch central, identificado con el circulo verde, será un Switch capa 3, que podrá ejecutar procesos de enrutamiento que disminuyan el trabajo del enrutador.

Se proponen instalar puntos de acceso (estándar IEEE 802.11) que puedan distribuir el servicio de internet en varios lugares de la empresa, estos puntos de acceso se harán formar parte solo de la VLAN que da salida a internet. Es posible realizar un filtrado a través de las direcciones MAC (dirección física) de los equipos a los cuales se desea dar acceso en el dispositivo. Este punto de acceso puede ser un Enrutador común configurado como tal.

### 4.3 Dimensionamiento de ancho de banda

Luego del levantamiento de información en cada una de las sedes se estimó el ancho de banda necesario para el intercambio de datos entre ellas. Para dimensionar este ancho de banda los parámetros considerados fueron los siguientes: cantidad de equipos como computadoras, impresoras, servidores, que tendrán acceso a los servicios. También se tomó en cuenta que las aplicaciones a utilizar por los usuarios de la red no requieren altas velocidades de transferencia de datos, como podría ser el caso de una red para video.

La transferencia de datos desde internet se ejecuta en ráfagas, esto quiere decir que no consumen constantemente recursos del canal. El nivel de concurrencia, que se refiere a la cantidad de tiempo efectivo de utilización del canal, en el caso de estudio, es muy baja por lo que los requerimientos de ancho de banda no son muy elevados.

A fin de expresar un valor numérico para el ancho de banda se presenta a continuación unos cálculos de un dimensionamiento tomando un factor de concurrencia del 100 por ciento, aunque este factor no es real se tomara de esta manera para dar holgura a servicios futuros y tener escalabilidad.

Este cálculo se realizó de la siguiente manera:

***Las Mayas***

Siendo el nodo central ya está casi totalmente consolidado en cuanto a cantidad de personal se refiere, por lo que se estipula que no existirá un crecimiento notable.

(32 Kbps x 75 usuarios) x 1 = **2400 Kbps**

***Zona Rental***

Esta sede se encuentra en un edificio compartido por lo que no posee mucho espacio físico para su expansión, se considera un crecimiento del 30 %.

(32 Kbps x 29 usuarios) x 1,3 =**1206,4 Kbps**

***Artigas***

No se espera un crecimiento tan notable en esta localidad, por lo que se estima un crecimiento del 30 %.

(32 Kbps x10 usuarios) x 1,3 = **416 Kbps**

***La Yaguara***

Actualmente esta localidad se encuentra en desarrollo, se están construyendo nuevas oficinas con lo que se espera un aumento de usuarios, se proyecta un crecimiento de 100 %.

(32 Kbps x22 usuarios) x 2 = **1408 Kbps**

Se considera una velocidad de 32 Kbps, porque los servicios y aplicaciones como los sistemas o correo electrónico no requieren ancho de banda especialmente elevado. Mayormente es destinado a la descarga de correos electrónicos, los cuales tienen un tamaño aproximado de 2 Mb, teniendo con esto un tiempo necesario de poco más de un minuto para la descarga si se garantiza esta velocidad a todos los usuarios.

Existen usuarios especiales que necesitan mayor velocidad para llevar a cabo su trabajo de manera más eficiente, éstos deben ser tomados en cuenta en el momento de la configuración de los equipos que administren el ancho de banda.

Se presenta a continuación la tabla 4-1, con las velocidades para la descarga de datos desde internet, asignados a cada uno de las sedes.

**Tabla 4-1.** ***Velocidad de descarga de internet***

| Sede | Ancho de Banda del enlace |
|---|---|
| **Las Mayas** | 2 Mbps |
| **Artigas** | 1 Mbps |
| **Zona Rental** | 1 Mbps |
| **La Yaguara** | 2 Mbps |

Es importante destacar que estos cálculos no están basados en alguna fórmula definida, sino más bien en una propuesta basada en observaciones del comportamiento de la red durante la descarga de datos desde internet.

**Tabla 4-2.** ***Ancho de Banda para Enlaces entre las sedes y el nodo central***

| Sede | Ancho de Banda del enlace |
|---|---|
| **Artigas** | 2 Mbps |
| **Zona Rental** | 2 Mbps |
| **La Yaguara** | 2 Mbps |

La tabla 4-2 se muestra el ancho del canal para las interconexiones entre el nodo central (Las Mayas), con las demás sedes. Este ancho se estima un poco mayor

a la necesidad de la velocidad de descarga considerando que existirán aplicaciones propias de la red que necesitaran este camino para el intercambio de datos.

Para controlar el ancho de banda será necesario un equipo o un software que se encargue de la tarea de distribuir las velocidades de navegación en las sedes. Esta configuración puede estar disponible en ciertos Enrutadores, también existen equipos servidores exclusivos para esta tarea.

# CAPITULO V

## EQUIPOS Y CONFIGURACIONES

### 5.1 Selección de equipos y proveedores de servicio

Luego de plantear el diseño de las redes de acuerdo a las necesidades de la empresa es necesario definir el proveedor de servicios y los equipos necesarios para implementar las redes.

#### 5.1.1 Proveedores de servicios

Como proveedor principal de servicio se considerar la empresa CANTV, como la más adecuada para dar respuesta a las necesidades de la red. Esta empresa cuenta con la infraestructura más completa a nivel nacional comparada con cualquier otro proveedor, lo que presenta una ventaja al momento de interconectar las localidades ubicadas en distintas zonas de la ciudad.

El *backbone* de CANTV cuenta con varios anillos de fibra conectados entre sí, que permite lograr los enlaces entre las sedes a través de Switches localizados cerca de las áreas donde se necesita la conexión.

CANTV, además de ofrecer los servicios de conexión, posee departamentos de ventas de equipos de comunicaciones, ofreciendo de esta manera la facilidad de adquirir los dispositivos adecuados para la tecnología que se maneja. Aunado a esto, los precios que ofrecen son altamente competitivos en el mercado.

### 5.1.2 Equipos

En esta sección se presenta la selección de los equipos según los diseños presentados anteriormente. Se hará una diferenciación entre los equipos para la implementación de la LAN y los necesarios para la WAN. También se colocaron los equipos que la empresa ya posee, con la aclaratoria correspondiente.

#### 5.1.2.1 Red Local nodo central (LAN)

Los switches administrables de las áreas alejadas del centro de datos pueden ser de cualquier tipo o marca de switch que cumpla con características de capa 2. Se propone un **GS-1548** marca **Zyxel**: este switch cumple con las especificaciones necesarias y tiene un precio moderado comparado con otros en el mercado, serian necesario 3 dispositivos como este.

Para el Switch central de la red local se propone utilizar un dispositivo que ya existe en la empresa por lo que no se incurriría en un gasto adicional. Este Switch es un **Cisco 3500-series Catalyst**, este dispositivo tiene características de capa 3, por lo que puede desempeñar funciones de enrutamiento y listas de acceso, reduciendo así la carga a los otros dispositivos como los Enrutadores.

Para los puntos de acceso inalámbrico (***access point***), pueden ser utilizados Enrutadores inalámbricos D-LYNK, configurados como puntos de acceso y no como enrutador. Estos dispositivos se encuentran en el inventario de la empresa.

#### 5.1.2.2 Red de área amplia (WAN)

Es necesario un Enrutador en cada sede capaz de manejar las velocidades adecuadas para la conexión WAN. Se plantea utilizar un **Cisco 2901.** Este dispositivo

lo ofrece CANTV para el manejo de sus servicios de MetroEthernet, por lo que no habría problemas de compatibilidad con los servicios solicitados. Será necesario un Enrutador (Cisco 891) o un Switch capa 3 por sede siendo 3 en total, el central que se encargue del manejo del tráfico hacia internet

Para la protección de la WAN es necesario un Firewall, este equipo además de brindar protección contra ataques a la red, permite también la creación de la DMZ. Como se expuso anteriormente, este tipo de configuración permitirá ofrecer servicios desde internet sin poner en riesgo la red privada. Existen Firewall tanto en hardware como software, las ventajas que atañen uno u otro son discutibles.

Un firewall en hardware ofrecerá mayor cantidad de servicios y protección, pero también su costo es más elevado. En la red es necesario un nivel de seguridad intermedio, ya que existen procesos que implican manipulación de recursos económicos, por esto es recomendable invertir en la adquisición de este equipo para lograr dicha protección. Para ello se sugiere el siguiente equipo: 320 Fortigate.

Es necesario para cada una de las sedes al menos un Switch administrable de cualquier marca, en el cual sea posible la creación de VLANs (capa 2). A continuación se presenta una tabla totalizando los equipos precisos para implementar todos los diseños propuestos, tanto la red WAN como la red LAN del nodo central.

Para lograr distribuir la velocidad de descarga de acuerdo a la tabla 4-1, se propone utilizar un controlador de ancho de banda. Este equipo se dedicara exclusivamente a separar los 6 Mb de la conexión de internet en ancho de banda independiente para cada sede, como se determinó en el dimensionamiento en la sección 4.3. Con este dispositivo puede limitarse al ancho de banda por usuario y de esta manera contribuir con la optimización del uso de este recurso.

**Tabla 5-1.** ***Totalización de equipos***

| Equipos | Modelo | Cantidad |
|---|---|---|
| **Switch capa 2** | GS-1548 Zyxel | **3** |
| **Switch capa 3** | Cisco 3500-series Catalyst | **1** (ya en la empresa) |
| **Switch no administrable** | 3com | **3** **(**ya en la empresa**)** |
| **Enrutador** | Cisco 891 | **3** |
| **Enrutador** | Cisco 2901 | **1** |
| **Access Point** | Enrutador D-LYNK DIR-600 | **3** (ya en la empresa) |
| **Controlador Ancho de Banda** | - | **1** |
| **Firewall** | 320 Fortigate | **1** |

## 5.2 Propuesta de configuración de equipos

Las propuestas de configuración se plantean en una forma general, éstas no reflejan códigos ni configuraciones específicas para cada dispositivo. Sin embargo, se muestran a manera de ejemplo algunos códigos de configuración concernientes al diseño planteado (Ver anexos).

A continuación se presentan los parámetros necesarios a tomar en cuenta al momento de configurar los equipos, a fin de ser consecuente con el diseño propuesto. También se sugieren, en algunos casos, los tipos de protocolos que se utilizarán para el correcto desempeño de la red.

### 5.2.1 Configuración de VLAN

La creación de las VLANs se propone de la siguiente manera:

- **VLAN 2:** Gestión.
- **VLAN 3:** Registro y control.
- **VLAN 4:** Internet.
- **VLAN 5:** Nómina.
- **VLAN 6:** Romana.
- **VLAN 7:** Voz.

Con la creación de estas seis VLANs, dispuestas como se observa en la Figura 3-3, se restringirá o se dará acceso preferencial según el área de trabajo donde se desempeñen los equipos. Cada VLAN tendrá acceso exclusivamente a los servicios que sean necesarios para ésta, se logra así proteger los procesos críticos como lo son el de nómina, La Romana y recaudación.

La manipulación de estos servidores es muy delicada por el tipo de información que manejan, por lo que es indispensable protegerlos. A continuación se presenta una tabla con los accesos de acuerdo a las VLAN, y los departamentos que deben conformarla.

**Tabla 5-2.** ***Acceso VLANs***

| VLAN | ACCESO a SERV. | DEPARTAMENTOS |
|---|---|---|
| **2** | Todos | Tec. De Info. |
| **3** | Registro y control | Recaudación / Registro y control |
| **4** | Sólo internet | General/ puntos de acceso |
| **5** | Nómina | Nómina |
| **6** | La Romana | Registro y control/Operaciones |
| **7** | Serv. VoIP | Todos |

Para la comunicación entre las VLANs, se propone configurar el Switch capa 3 de manera tal que permita controlar el acceso entre ellas. Adicionalmente, para un mejor rendimiento de los equipos se plantea utilizar ACL.

La VLAN 1 no se utiliza debido a que se encuentra de forma predeterminada en lo Switches, y ésta se asigna automáticamente a los puertos que no tienen habilitada una VLAN.

### 5.2.2 Lista de acceso (ACL)

En esta lista se definen los accesos de las VLANs mostrados en la tabla 5-2. También se puede permitir a usuarios especiales acceder a servicios que sean necesarios para su desempeño laboral, mediante su dirección MAC o IP.

La lista de acceso puede ser configurada en el Firewall, con el fin de elevar el nivel de seguridad que requieran algunos servicios y no sobrecargar de procesos al Enrutador, o Switch capa 3 que también son capaces de crear listas de acceso.

### 5.2.3 Creación de subredes (Subneteo)

A continuación se presentan las tablas de subneteo, estas se construyeron a partir de la *Tabla 2-4*, tomando en cuenta la cantidad de usuarios que conformarían las subredes. La notación /24 indica la cantidad de bits con ´´1´´ que existen en la parte de la dirección IP que indica la red.

Para los nodos distintos al nodo central, en principio sólo se propuso una VLAN según la cantidad de usuarios en cada sede. Es posible configurar también en las sedes las mismas VLAN que existen en el nodo central.

En general la cantidad de usuarios por cada VLAN está alrededor de 20 usuarios, con excepción de La Romana y nómina que tienen máximo 10 usuarios. Para la VLAN de acceso a internet se propone dejar al menos 30 direcciones disponibles.

**Tabla 5-3.** ***Red Las Mayas (Nodo central)  IP: 192.168.10.0/24***

| Nombre de la sub-red | Dirección de Red | Rango de IP | | Host disponibles por subred | Mascara de Red | Broadcast |
|---|---|---|---|---|---|---|
| | | Desde | Hasta | | | |
| VLAN 2 | 192.168.10.0 | 192.168.10.1 | 192.168.10.30 | 30 | 255.255.255.224 | 192.168.10.31 |
| VLAN 3 | 192.168.10.32 | 192.168.10.33 | 192.168.10.62 | 30 | 255.255.255.224 | 192.168.10.63 |
| VLAN 4 | 192.168.10.64 | 192.168.10.65 | 192.168.10.94 | 30 | 255.255.255.224 | 192.168.10.95 |
| VLAN 5 | 192.168.10.96 | 192.168.10.97 | 192.168.10.110 | 14 | 255.255.255.240 | 192.168.10.111 |
| VLAN 6 | 192.168.10.112 | 192.168.10.113 | 192.168.10.126 | 14 | 255.255.255.240 | 192.168.10.127 |
| VLAN 7 (Red a Futuro) | 192.162.10.128 | - | - | - | - | - |

**Tabla 5-4.** ***Red Artigas IP: 192.168.11.0/24***

| Nombre de la sub-red | Nº de host a utilizar | Dirección de Red | Rango de IP | | Host disponibles por subred | Mascara de Red | Broadcast |
|---|---|---|---|---|---|---|---|
| | | | Desde | Hasta | | | |
| **VLAN 11 Artigas** | **10** | **192.168.11.0** | **192.168.11.1** | **192.168.11.30** | **30** | **255.255.255 .224** | **192.168.10.31** |
| **Red a Futuro** | **-** | **192.168.11.32** | **-** | **-** | **-** | **-** | **-** |

**Tabla 5-5.** ***Red Yaguara IP: 192.168.12.0/24***

| Nombre de la sub-red | Nº de host a utilizar | Dirección de Red | Rango de IP | | Host disponibles por subred | Mascara de Red | Broadcast |
|---|---|---|---|---|---|---|---|
| | | | Desde | Hasta | | | |
| **VLAN 12 Yaguara** | **22** | **192.168.12.0** | **192.168.12.1** | **192.168.12.62** | **62** | **255.255.255. 192** | **192.168.12.63** |
| **Red a Futuro** | **-** | **192.168.12.64** | **-** | **-** | **-** | **-** | **-** |

**Tabla 5-6.** ***Red Zona Rental IP: 192.168.13.0/24***

| Nombre de la sub-red | Nº de host a utilizar | Dirección de Red | Rango de IP | | Host disponibles por subred | Mascara de Red | Broadcast |
|---|---|---|---|---|---|---|---|
| | | | Desde | Hasta | | | |
| **VLAN 13 Zona Rental** | **20** | **192.168.13.0** | **192.168.13.1** | **192.168.13.62** | **62** | **255.255.255. 224** | **192.168.13.63** |
| **Red a Futuro** | **-** | **192.168.13.64** | **-** | **-** | **-** | **-** | **-** |

### 5.2.4 Enrutamiento

Debido a la cantidad de nodos que tiene la WAN, y por la topología estrella seleccionada, se puede configurar el enrutamiento en modo estático en los Enrutadores de borde así como en el Enrutador central. Éste se encargará de distribuir todos los recursos, de esta manera se definen los caminos lógicos necesarios para las interconexiones.

Se plantea el enrutamiento en modo estático para evitar el procesamiento innecesario en los Enrutadores. Todos los caminos de datos no variables se crearán a través del Enrutador central por lo que no es necesario un protocolo de enrutamiento que defina dichos caminos.

Este enlace, para efectos de los Enrutadores de la red WAN, es *visto* como un enlace punto a punto, por lo que existe un único camino entre los Enrutadores de borde y el Enrutador central.

A cada Enrutador de borde en cada una de las sedes, se debe configurar de la siguiente manera: todas las peticiones de su red LAN dirigidas hacia internet, deben enviarse al proxy caché en la sede, y de no encontrar los objetos buscados debe enviarse la petición al Enrutador central de la red WAN (Las Mayas). Las peticiones no dirigidas a internet irán directamente al Enrutador central.

El Enrutador de Las Mayas tendrá asignado en cada puerto una única dirección de red, asociada a una única sede y éste direccionará todas las peticiones hacia el firewall. Este equipo se encargará de permitir o denegar dicha petición de acuerdo a la lista de acceso configurada en el Firewall. Esto lo hará tanto para las peticiones de páginas de internet como aquellas que son dirigidas a los servicios alojados en los servidores del nodo central.

## 5.3 Solución CANTV

Se solicitó a CANTV los enlaces entre las sedes para hacer posible la implementación de la red WAN. La propuesta de CANTV plantea una solución en metro-cobre. Estos enlaces dedicados son configurados como *tuberías* virtuales que interconectan las sedes. Para el acceso a internet se solicitan direcciones IP públicas fijas, y una velocidad de 6 MB para este servicio, que es suficiente según el dimensionamiento realizado en la sección 4.3.

El servicio de internet será administrado desde un nodo central que se encargará de repartir la velocidad según sea la necesidad de cada sede, por lo que también se solicitaron enlaces punto a punto desde Las Mayas (Nodo central), hacia La Yaguara, Artigas y Zona Rental, a fin de interconectar las sedes a la red.

### Descripción del Producto Conectividad Metro Ethernet

**Concepto:**

Servicios de transmisión de datos que utiliza el estándar de transmisión Ethernet, el cual permite conectar localidades remotas o redes geográficamente separadas como si estuvieran en una misma LAN.

**Atributos Básicos:**

- VPN capa 2 con opciones de ancho de banda garantizado
- Servicios punto a punto, multipunto y acceso a Internet.
- Interfaces de acceso de 2 Mbps hasta 8 Mbps.
- Anchos de banda garantizados desde 1 Mbps hasta 8 Mbps.
- Última milla: cobre, dependiendo de la velocidad de conexión solicitada y la disponibilidad de medios de planta externa existentes.

- Fácil aprovisionamiento de localidades, servicios e incrementos de anchos de banda.

**Arquitectura Metro Ethernet Red Cantv**

- Switches Alcatel configurados con MPLS, interconectados en arquitectura de anillos vía fibra y sistema DWDM.
- Los servicios MetroEthernet están implantados de manera exclusiva en la red MetroEthernet y no utilizan al Backbone IP de Cantv.
- Utilizando MPLS en la Red Metro Ethernet se proveen servicios VPN de Capa 2, contando con dos mecanismos de transporte Ethernet basados en MPLS:
    - VLL: para conexiones Ethernet punto a punto
    - VPLS: para conexiones Ethernet punto a multipunto

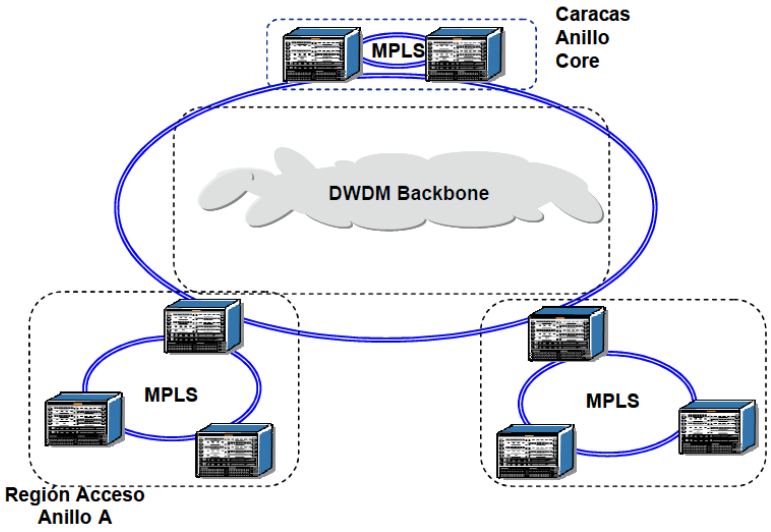


**Figura 5-1.** ***Topologías CANTV***

**Fuente:** ***CANTV***

**Conectividad Metro VPLS**

**Características**

- Utiliza switches MPLS para construir VPNs en capa 2.
- Las VPNs de capa 2 permiten a los clientes ver su red como una LAN.
- A diferencia de las VPNs de capa 3 el cliente puede utilizar un direccionamiento IP/Enrutamiento propio a conveniencia, manteniendo el control del mismo.
- Las VPNs pueden ser punto-a-punto (VLLs) o multipunto (VPLS).
- Provee calidad de servicio (QoS) para la diferenciación del tráfico a nivel de capa 2 en las VPNs.
- Es una red de transporte utilizando topología de anillos.

Esta propuesta de CANTV satisface las necesidades para la conexión WAN de SUPRA-Caracas. Con esta capacidad de interconexión la implementación de la red es alcanzable, y todos los servicios planteados así como las configuraciones son compatibles con la plataforma.

# CONCLUSIONES

A partir de los avances en las redes de computadoras, que tienen origen en la década de los 60, así como los primeros sistemas de internet, todas las actividades humanas se han ajustado para obtener beneficios de estos nuevos modelos de comunicación. En este proyecto se realizó un diseño a través del cual la empresa SUPRA podrá contar con una plataforma de comunicaciones eficiente y que le servirá para mejorar todos sus procesos y agilizar la distribución y propagación de información relevante.

Para el diseño de estas redes se tomaron en cuenta aspectos tales como las actividades y dinámica que la empresa desarrolla, la distribución física de las sedes, cantidad de usuarios y los servicios necesarios para un mejor desempeño de sus trabajadores. De esta manera se ofrece una solución completa que satisface las necesidades de la compañía. Los diseños planteados en este proyecto son realizables, ya que la empresa posee los recursos. Además, los equipos y la tecnología necesarios para la implementación están disponibles en el mercado

La interconexión de las distintas sedes en una red WAN con topología estrella, permitirá que todas las sedes estén virtualmente en el mismo lugar que el centro operativo de la empresa, haciendo posible la comunicación directa con éste. Cuando los procesos que involucran el desempeño de las labores de los trabajadores de la empresa se ven mejorados, también se ve mejorado el desempeño general de la misma, por esto con la implementación del diseño el funcionamiento de la empresa será más eficiente, se conocerán y solventaran los problemas de manera expedita ya que la información circulará por las sedes de forma rápida.

Al momento de dimensionar el ancho de banda no se encontró una regla general para su cálculo. El tráfico en las redes de datos funciona en ráfagas, con la ocurrencia de eventos aleatorios y dependen de muchos factores externos como internet. Comúnmente al ancho de banda se determina de acuerdo a los servicios que se transportarán en el canal de comunicación. En este trabajo el criterio utilizado fue basado en la velocidad para la descarga de 32 Kbps, considerado esta una velocidad suficiente para el tipo de actividades que desarrolla los usuarios de la red de la empresa.

Es importante que además de un dimensionamiento adecuado del ancho de banda, se implementen soluciones que disminuyan el tráfico, con lo cual la red se desempeñará de forma óptima. Es por esta razón que al diseño se agregaron equipos como: el controlador de ancho de banda y los servidores Proxy Caché en cada una de las sedes. Sin el proxy todas las peticiones deberían viajar hasta el Enrutador central, lo que consumiría ancho de banda, y sin el controlador de ancho de banda no se podría distribuir la velocidad de descarga según las necesidades de cada sede.

Con la creación de VLANs se crean dominios de difusión que confinan las peticiones de los equipos a una sola subred, evitando así el tráfico innecesario en nodos que no contengan el destino de la petición. Esto se traduce en una mejora en el desempeño de la red, generando beneficios como: menor tráfico broadcast, seguridad en las subredes, separación de servicios, etc.

La implementación de esta red permitirá el funcionamiento de servicios como: asistencia remota, Video sobre IP para vigilancia a distancia, acceso a base de datos, y en especial VoIP que, de funcionar en la red PSTN, sería muy costoso y no administrable. Lo que aportará una notable mejora en el desempeño general de la institución.

# RECOMENDACIONES

A medida que la red de la empresa vaya creciendo la cantidad de usuarios de la red se incrementará, por lo que se recomienda descentralizar algunos servicios, lo que permitirá un mejor uso del canal comunicaciones. El hecho de que todos los servicios deban ser accedidos en el mismo nodo generará un embotellamiento que tendrá como consecuencia un deterioro notable de la calidad del servicio.

Con el crecimiento de la cantidad de usuarios y aplicaciones, será necesaria la implementación de calidad de servicio (QoS), que se refiere a la habilidad de proporcionar una prioridad distinta a diferentes aplicaciones manteniendo así, cierto nivel de rendimiento en el flujo de datos.

Aplicaciones específicas como VoIP requieren de QoS, cuando se cuanta con recursos y ancho de banda limitados. Es importante destacar que aunque en este proyecto se tomó en consideración la cantidad de usuarios para VoIP, no se analizaron a profundidad las necesidades de la red para soportar y cubrir el servicio, por lo que se recomienda un estudio dedicado a este tema que abarque todas las variables que puedan influir en su futura implementación.

Al momento de la implementación de la red pueden surgir errores técnicos que disminuyen la calidad de la comunicación. A continuación se presentan algunos consejos a tomar en cuenta en el momento de la instalación del cuarto de datos y del cableado, lo que ayudará a prevenir fallas en la capa física:

***Para el cuarto de datos:***

- Las paredes deben tener pintura contra incendios.
- El piso preferiblemente debe ser de goma de manera de mantener aislados los equipos.
- El cuarto debe contar con una puesta a tierra, adecuada a los requerimientos de los equipos.
- Debe contar con aire acondicionado y así mantener una temperatura ideal para el funcionamiento adecuado de los dispositivos.

***Al momento de realizar el cableado se debe tener en cuenta:***

- No desenredar los pares trenzados, que están dentro del UTP, más de una pulgada y media antes de insertarlos en el conector RJ-45.
- No dejar más de 2,5 cm expuesto (desnudo) el cable antes de la terminación. Si se hace, aumentará la posibilidad de interferencias y errores de datos.
- Observar y cumplir las limitaciones radio de curvatura para el tipo de cable que se está instalando. El radio de curvatura es el radio del arco máximo en el cual puede circular un cable antes de alterar la transmisión de datos. Generalmente, el radio de un cable de par trenzado de curvatura es igual o mayor que cuatro veces el diámetro del cable.
- Utilizar un analizador de cables para verificar que cada segmento de cableado se instala transmite los datos de manera fiable. Esta práctica evitará que más tarde se tenga que localizar errores en tramos largos de cable.
- Evitar apretar los cables con mucha fuerza ya que puede maltratar su cubierta exterior, y ocasionar errores difíciles de detectar.
- Evitar el tendido de cables por el suelo donde podría sufrir daños de sillas rodantes o tráfico de pie. Si se tiene que tomar este camino, cubra el cable con un protector de cable.

- Instalar el cable por lo menos a un metro de distancia de luces fluorescentes o de otras fuentes que puedan ocasionar interferencia. Esto reducirá la posibilidad de que el ruido afecte a las señales de su red.
- Dejar siempre una cierta holgura en tendidos de cable. Instalar cables con demasiada tensión expone a la red a problemas de conectividad y transmisión de datos.
- Cumplir con los requisitos de conexión a tierra de los equipos a instalar.

# REFERENCIAS BIBLIOGRAFICAS


[1] Tamara Dean, "Networking Standards and the OSI Model," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 2, p. 57.

[2] TextosCientificos. (2006) Sitio Web Textos Cientificos.com. [Online]. http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi

[3] Tamara Dean, "An Introduction to Networking," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 1, p. 4.

[4] Tamara Dean, "An Introduction to Networking," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 1, p. 6.

[5] Tamara Dean, "An Introduction to Networking," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, p. 7.

[6] Tamara Dean, "An Introduction to Networking," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 1, p. 7.

[7] Tamara Dean, "Topologies and Ethernet Standards," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 5, p. 195.

[8] Tamara Dean, "Topologies and Ethernet Standards," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 5, p. 197.

[9] Tamara Dean, "Topologies and Ethernet Standards," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 5, p. 198.

[10] Tamara Dean, "Topologies and Ethernet Standards," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 5, p. 199.

[11] Tamara Dean, "Topologies and Ethernet Standards," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 5, p. 201.

[12] Tamara Dean, "Topologies and Ethernet Standards," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 5, p. 201.

[13] Tamara Dean, "Topologies and Ethernet Standards," in *Network+ Guide to*

*Networks*, 5th ed. Boston: Course Technology, 2009, ch. 5, p. 202.

[14] Tamara Dean, "Introduction to TCP/IP Protocols," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 4, p. 162.

[15] Tamara Dean, "Introduction to TCP/IP Protocols," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 4, p. 162.

[16] INTEF. (2006) Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado. [Online]. http://www.ite.educacion.es/es/intef

[17] JAVA. (2003) Java. [Online]. http://www.java.com/es/download/help/proxy_server.xml.

[18] Antonio Huerta. (2010, Marzo) Security Artwork. [Online]. http://www.securityartwork.es/2010/03/03/servidores-proxy-cache-%E2%80%93-optimizando-la-red/

[19] VIA SERVER CENTER. (2006) Via Server Center. [Online]. http://viaservercenter.com/index.php?option=com_content&task=view&id=13&Itemid=28.

[20] VOIPES. (1999) VoIPes. [Online]. http://www.voipes.info/

[21] Tamara Dean, "Introduction to TCP/IP Protocols," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 4, p. 138.

[22] Tamara Dean, "Introduction to TCP/IP Protocols," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 4, p. 142.

[23] Tamara Dean, "Introduction to TCP/IP Protocols," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 4, p. 142.

[24] Tamara Dean, "Introduction to TCP/IP Protocols," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 4, p. 147.

[25] Tamara Dean, "In-Depth TCP/IP Networking," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 10, p. 487.

[26] Tamara Dean, "In-Depth TCP/IP Networking," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 10, p. 488.

[27] Tamara Dean, "In-Depth TCP/IP Networking," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 10, p. 489.

[28] Tamara Dean, "In-Depth TCP/IP Networking," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 10, p. 490.

[29] Tamara Dean, "In-Depth TCP/IP Networking," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 10, pp. 497-499.

[30] Tamara Dean, "Network Hardware," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 6, p. 270.

[31] Tamara Dean, "Network Hardware," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 6, p. 272.

[32] Tamara Dean, "Network Hardware," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 6, p. 273.

[33] Tamara Dean, "Topologies and Ethernet Standards," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 5, p. 207.

[34] Alejandro Castro, Gerardo Gonzalez, Robert Montenegro, and Evelio Fuenmayor, "Redes de banda Ancha: Metro Ethernet," Maracaibo-Edo. Zulia, 2009.

[35] Tamara Dean, "WANs and Remote Connectivity," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 7, p. 336.

[36] Tamara Dean, "Transmission Basics and Networking Media," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 3, pp. 97-100.

[37] Tamara Dean, "Transmission Basics and Networking Media," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 3, p. 101.

[38] Tamara Dean, "Transmission Basics and Networking Media," in *Network+ Guide to Networks*, 5th ed. Boston: Course Technology, 2009, ch. 3, pp. 106-107.

# BIBLIOGRAFÍA


Arias, F. (2006). *El Proyecto de Investigación. Introducción a la metodología científica.* Caracas: Episteme.

Arjona, V. (2011). *Propuesta de red de comunicaciones bajo la plataforma metro Ethernet de CANTV para la interconexión de las unidades navales de la Armada Bolivariana en la zona metropolitana.* Trabajo Especial de Grado, Universidad Central de Venezuela, Caracas.

Aveledo, A. (1994). *Desarrollo de una red metropolitana de transmisión de datos para la Bolsa de Valores de Caracas.* Trabajo de Grado, Universidad Central de Venezuela, Caracas.

Cisco Networking Academy. (2009). *CCNA Exploratoria 4.0 Aspectos Básicos de Networking.*

Dean, T. (2009). *Network+ Guide to Networks* (5ta. Edición ed.). Boston: Course Technology.

Gagliano, R. (2003). *VPLS sobre un Backbone MLPS.* Tesis.

García, G. (s.f.). Recuperado el Junio-Octubre de 2012, de Gastoncracia: http://www.garciagaston.com.ar/

IEEE. (s.f.). Recuperado el Julio de 2012, de IEEE, Advancing Technology for Humanity: http://www.ieee.org/about/index.html

MICROSOFT. (s.f.). Recuperado el Abril de 2012, de Sitio Web de Soporte Técnico Microsoft: http://www.support.microsoft.com

UNA. (2010). *Red LAN para el centro local de Amazonas.* Tesis, Universidad Nacional Abierta, Puerto Ayacucho.

WIKIPEDIA. (s.f.). Recuperado el Abril-Octubre de 2012, de Wikipedia, la Enciclopedia libre: http://www.wikipedia.com

# ANEXOS

Configuración de rutas estáticas..... 2

Configuración de VLAN..... 3

Especificaciones Router CISCO 2901 ..... 4

Configuración de puertos troncales ..... 5

# ANEXO 1

## Configuración de rutas estáticas

Las rutas estáticas se configuran mediante el comando **ip route** en la consola de los enrutadores, en el **modo configuración global**, utilizando la siguiente sintaxis:

**Router(config)# ip route « *IP destino + máscara de red destino ó subred destino* » « *IP del siguiente salto ó interfaz de salida* » « *distancia administrativa* »**

**IP destino + máscara de red o subred destino:** La IP específica la red o host que se quiere alcanzar junto con la máscara de red o subred correspondiente.

**IP del siguiente salto:** Es la IP de la interfaz del router conectado directamente al router donde se está configurando la ruta estática.

**Interfaz de salida:** Es la interfaz serial del router donde se está configurando la ruta estática. Se utiliza en el caso de desconocer la IP del siguiente salto.

**Distancia administrativa:** Si no se especifÍca distancia administrativa, esta tomará el valor por defecto de 1 en la tabla de enrutamiento. El valor puede ser de 1-255, siendo 1 el valor que da más importancia a la ruta.

# ANEXO 2

## Configuración de VLAN

A continuación se presenta un ejemplo de configuración de VLAN en un Switch.

```
S1# vlan database
S1# vlan 10
S1# name salon
S1# vlan 20
S1# name alumnos
S1# vlan 99
S1# name admin
S1# exit

S1# configure terminal
S1(config)# interface vlan 99
S1(config)# ip address 192.168.99.2 255.255.255.0
S1(config)# no shutdown
S1(config)# exit
S1(config)# ip default-gateway 192.168.99.1
S1(config)#interface range fastEthernet 0/3 - 9
S1(config-if-range)#
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
```

Para realizar el modo trunk entre los dos switch se debe usar el siguiente comando en la interface que interconecta los dos switches.

```
S1(config)#interface fastEthernet 0/1
S1(config-if)#switchport mode trunk
```

# ANEXO 3

## Especificaciones Router Cisco 2901

| General | |
|---|---|
| Tipo de dispositivo | Enrutador |
| Tipo de conectividad | Cableada |
| Protocolos de transmisión de datos | Ethernet, Fast Ethernet, Gigabit Ethernet |
| Protocolos de enrutamiento | OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, enrutamiento estatico IPV4,enrutamiento estatico IPv6 , (PBR) |
| Protocolo para administración remota | SNMP, RMON |
| Propiedades | Firewall , soporta VPN , MPLS, soporta Syslog , soporta IPv6 , *Class-Based Weighted Fair Queuing* (CBWFQ), *Weighted Random Early Detection* (WRED) |
| Estándares complementarios | IEEE 802.1Q, IEEE 802.3af, IEEE 802.3ah, IEEE 802.1ah, IEEE 802.1ag |
| RAM | 512 MB (instalada) / 2 GB (max) |
| Memoria Flash | 256 MB (instalada) / 8 GB (max) |
| **Expansión / Conectividad** | |
| Interfaces | 2 x 10Base-T/100Base-TX/1000Base-T - RJ-45 ¦ Management : 1 x console - RJ-45 ¦ Management : 1 x console - mini-USB Type B ¦ Serial : 1 x auxiliary - RJ-45 ¦ USB : 2 x 4 PIN USB Type A |
| Slots libres para expansión | 4 ( 4 ) x EHWIC ¦ 2 ( 2 ) x PVDM ¦ 2 ( 1 ) x CompactFlash Card ¦ 1 ( 1 ) x ISM |
| **Alimentación** | |
| Voltaje requerido | AC 120/230 V ( 50/60 Hz ) |
| **Misceláneos** | |
| Espesor | 43.8 cm |
| Profundidad | 43.9 cm |
| Altura | 4.5 cm |
| Peso | 6.1 kg |
| **Software** | |
| Proveedor OS | Cisco IOS IP Base |
| **Parámetros ambientales** | |
| Temp. mínimo operativa | 0 °C |
| Temp. máxima operativa | 40 °C |
| Rango de humedad | 10 - 85% |

# ANEXO 4

## Configuración de puertos troncales

Un puerto troncal es un enlace punto a punto que envía y recibe tráfico entre switches, o entre switches y routers.

Los puertos troncales pueden transportar el tráfico de múltiples VLANs y pueden extender las VLANs a través del toda la red. Los puertos troncales (100Base-T y Gigabit Ethernet) utilizan el protocolo propietario de Cisco Inter-Switch Link (ISL), como protocolo predeterminado, o el protocolo estándar de la industria IEEE 802.1Q, para transportar el tráfico de las múltiples VLAN sobre un solo enlace.

Los puertos troncales que utilizan el protocolo IEEE 802.1Q tienen las siguientes limitaciones:

Si la VLAN nativa en un extremo del enlace troncal es diferente a la VLAN nativa en el otro extremo, se pueden generear loops del protocolo Spanning-Tree Protocol (STP). Por lo tanto, la VLAN nativa para un enlace troncal utilizando 802.1q debe ser la misma en ambos extremos del puerto troncal.

Después de que se ingrese al modo de *enable*, completar los siguientes pasos para los switches Catalyst 3500XL Series:

1. Ingresar al modo de configuración global ingresando el comando **configure terminal**.

2. Ingresar al modo de configuración de la interfaz e ingresar el comando **interface** [*type*] <*mod/port*> para ingresar el puerto que se agregará a la VLAN.

3. Ingresar el comando **switchport mode trunk** para configurar el puerto como troncal VLAN.

4. Ingresar el comando **switchport trunk encapsulation** [isl|dot1q] para configurar el puerto para que soporte la encapsulación ISL o bien 802.1q. Se debe configurar cada extremo del link con el mismo tipo de encapsulación. Si usted elige 802.1q, usted debe elegir una VLAN predeterminada para el puerto troncal.

5. Ingrese el comando para configurar la vlan nativa **switchport trunk native vlan** [*vlan-id*]. Este VLAN enviará y recibirá el tráfico sin etiquetas en el puerto troncal 802.1q. El rango valido para los identificadores de la VLAN (VLAN ID) es del 1 a 1001.

6. Ingresar el comando **end** para volver al modo EXEC privilegiado.

7. Ingrese el comando **show interfaces** *[type]* <*mod/port*> **switchport** para verificar sus configuraciones. En el resultado del comando, verifique los campos **Operational Mode** (Modo operativo) y **Operational Trunking Encapsulation** (Encapsulado operativo de conexión de troncal).

8. Ingrese el comando **copy running-config startup-config** para salvar la configuración.

Por defecto, un puerto troncal envía y recibe el tráfico de todas las VLANs que se encuentran configuradas en las bases de datos. Todos las VLANs son desde 1 a 1005.