# MEJORAMIENTO DEL RENDIMIENTO DE LA RED DE UN CLIENTE APLICANDO LAS POLITICAS DE DISEÑO DE CISCO SYSTEM

**JORGE ALBERTO BELEÑO GÓMEZ**

**UNIVERSIDAD SANTO TOMÁS**
**FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES**
**BOGOTÁ D.C.**
**2017**

# MEJORAMIENTO DEL RENDIMIENTO DE LA RED DE UN CLIENTE APLICANDO LAS POLITICAS DE DISEÑO DE CISCO SYSTEM

**Proyecto de Curso de Grado para optar el título de Ingeniero de Telecomunicaciones**


**Presentado Por:**

**JORGE ALBERTO BELEÑO GÓMEZ**

**Dirigido por:**

**GERALD BREEK FUENMAYOR RIVADENEIRA**
**Ingeniero de Sistemas**



**UNIVERSIDAD SANTO TOMÁS**
**FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES**
**BOGOTÁ D.C.**
**2017**

# Resumen

*La siguiente monografía documenta el diseño y la configuración de la red de un cliente de telecomunicaciones, se procede a realizar un análisis de todos los elementos que la componen para luego plantear una propuesta que busca mejorar el rendimiento de la red utilizando los parámetros de diseño y configuración que propone Cisco System, en sus cursos de certificación Cisco Certified Network Professional (CCNP).*

## Palabras Clave

*VLAN, LAN, Cliente, Calidad, Mejoramiento, Red, Diseño, Protocolos de enrutamiento, Switching, Enrutamiento.*

# Abstract

*The following monograph documents the design and configuration of a telecommunication client's network, an analysis of all the elements that compose it, and then a proposal that seeks to improve the performance of the network using the design parameters and Configuration offered by Cisco System in its Cisco Certified Network Professional (CCNP) certification courses.*

## Keywords

*VLAN, LAN, Client, Quality, Improvement, Network, Design, Routing Protocols, Switching, Routing.*

# Tabla de Contenidos

# Tabla de Figuras

# Índice de Tablas

# PARTE I

Introducción a la Investigación

# **CAPÍTULO 1**
# INTRODUCCIÓN A LA INVESTIGACION.

*En este capítulo se plantea la problemática actual de la red de telecomunicaciones, la justificación y los objetivos para realizar la propuesta de mejoramiento de la red de un cliente de telecomunicaciones.*

## 1.1. DESCRIPCIÓN DEL PROBLEMA

Para el diseño de una red de telecomunicaciones existen factores como normas, protocolos, topologías de red, entorno físico, equipos y costos que se deben tener en cuenta para determinar los componentes y las configuraciones más apropiadas a la hora de implementar los diferentes servicios que un cliente necesite, principalmente, la transferencia de datos y voz entre las diferentes sedes; El cliente de telecomunicaciones presenta una red básica que a su vez soporta mucho tráfico de datos entre todos los usuarios que la conforman, lo cual puede generar retrasos en el envío y la entrega de paquetes debido al mal diseño, distribución de los servicios y una mala planificación sobre el crecimiento de la red.

La red del cliente de telecomunicaciones que se presenta en el documento, cuenta con 9 sedes ubicadas en diferentes puntos de la ciudad y un *datacenter* en una de las sedes, todas interconectadas por fibra óptica a través de otro operador local. La red del cliente posee diferentes VLAN en cada sede y se comunican sí mediante enrutamiento interVLAN, por lo que no es necesario ningún protocolo de enrutamiento activo.

Tener una red de capa 2 conlleva muchas ventajas, incluyendo costos más bajos, solo requiere *switching*, no utiliza equipos de enrutamiento los cuales son más costosos, y ofrece una latencia muy baja, sin embargo la falta de enrutamiento crea desventajas en redes de capa 2 tales como tormentas de *broadcast*, una sobrecarga administrativa adicional de mantenimiento y de asignaciones IP debido a las subredes de los múltiples sitios y un reenvío de trafico constante de difusión, sobre todo de ARP y DHCP, es decir, cualquier trafico transmitido a un dispositivo se reenvía a todos los dispositivos y cuando la red se hace demasiado grande el tráfico de difusión comienza a crear congestiones y *loops* lo cual disminuye la eficiencia de la red, por estas razones, la red se encuentra comprometida para un futuro crecimiento en temas de escalabilidad y es necesario crear un plan de mejoramiento.

### Antecedentes del problema

A continuación se hace referencia a aquellos trabajos de investigación que exponen información relacionada con el presente documento y que se tuvieron en cuenta para la realización del mismo.

I. **Contreras, W. (2008). Propuesta para el mejoramiento de la red LAN de la compañía Danone Alquería S.A. (Tesis de Pregrado). Universidad Santo Tomás, Bogotá D.C., Colombia.**

La Compañía Danone Alquería S.A., al observar deficiencias en su red LAN,

solicita a la firma Bercont Ltda, asesoría para poder solucionar los problemas que presentan en su red de Datos (Baja eficiencia, caídas de servicios, entre otros), lo que retrasa la ejecución de sus procesos y por tanto molestias a nivel interno.

Se realiza un estudio donde se puede enseñar de manera documentada a la compañía las causas y consecuencias para poder dar con una solución económicamente viable.

II. **Parra, A. (2014). Propuesta de mejoramiento del desempeño de la red de telecomunicaciones para la empresa Kamilion S.A. (Tesis de Especialización). Universidad Santo Tomás, Bogotá D.C., Colombia.**

Se documenta el diseño de la red de datos para la empresa Kamilion S.A. En la propuesta se da solución tecnológica para mejorar el desempeño de la red de telecomunicaciones de la empresa mediante metodología PMI (Project Manager Institute).

III. **Umasuthan, V.. (May 5, 2016). Protecting the Communications Network at Layer 2. Transmission and Distribution Conference and Exposition (T&D), 2016 IEEE/PES, 1, 5. Feb 15, 2017, De IEEE Base de datos.**

Este documento analiza las amenazas que pueden surgir cuando las redes no están protegidas en la Capa 2 y algunos de los métodos disponibles para mitigar estas amenazas.

IV. **Álvares, F., Barajas, J., Barrero, A. (2015). Comparaciones e Implementaciones de Tecnologías para las Redes Empresariales (Proyecto de Consultoría). Escuela Colombiana de Ingeniería Julio Garavito. Bogotá D.C., Colombia.**

Se presenta una consultoría acerca de las diferentes tecnologías que se usan en redes LAN para la solución de problemas puntuales de diferentes empresas estudiadas.

Presentada la problemática surge el siguiente interrogante:

¿Cómo se puede mejorar el rendimiento de la red actual del cliente, aplicando las tecnologías, configuraciones y recomendaciones que propone Cisco System, en su curso de certificación Cisco Certified Network Professional?

## 1.2. OBJETIVOS

### OBJETIVO GENERAL

- Generar una propuesta para el mejoramiento del desempeño de la red actual de un cliente de telecomunicaciones basadas en la aplicación de buenas prácticas de diseño de Cisco System en su curso de certificación CCNP.

### OBJETIVOS ESPECÍFICOS

- Analizar la configuración de la red actual para poder generar un diagnóstico del funcionamiento de la red.
- Identificar los problemas encontrados en la red basados en los parámetros de diseño y configuración de Cisco System.
- Proponer las diferentes mejoras que se encuentren en la red del cliente para dar solución a los problemas que se identifiquen.
- Refrendar la propuesta presentada mediante la validación por juicio de un experto en redes, para dar constancia que los cambios son los más apropiados.

## 1.3. JUSTIFICACIÓN

El cliente de telecomunicaciones que se presenta busca facilitar el acceso y uso de las telecomunicaciones, brindando servicios de televisión, telefonía local y celular e internet haciendo uso de la innovación y la calidad con el fin de prestar el mejor servicio a los consumidores finales comprometiéndose con el desarrollo de la sociedad donde está ubicada.

El tráfico de datos y las constantes peticiones de información que se requieren en los centros de servicios y oficinas administrativas del cliente de telecomunicaciones hace que la red se sature y que existan fallas continuas (caídas de servicios, retardo de peticiones, entre otros) ocasionando retrasos en la ejecución de las tareas administrativas y de atención al cliente. Por esta razón la siguiente monografía busca generar una propuesta para mejorar el rendimiento de la red del cliente, la cual está generando retrasos en la ejecución de sus tareas y se busca crear un plan de mejoramiento adaptado a las exigencias de los servicios y necesidades que el cliente requiere, presentando así un beneficio a la compañía y a la comunidad que adquiere los servicios que esta presta, de lo contrario la compañía puede perder demanda y quedar en desventaja frente a la competencia causando pérdidas económicas y de clientes.

El plan de mejoramiento presenta un beneficio económico a la compañía ya que en ningún momento se presenta una propuesta de inversión económica debido a que la infraestructura y equipos que posee no necesita cambios a nivel de hardware, todos los equipos utilizados ya existen dentro de la red del cliente y solo se hacen cambios a nivel de diseño y configuración.

El curso de Cisco System, CCNP brinda todas las herramientas necesarias para poder generar un plan de mejora a la red de datos de la compañía, convirtiéndose este en la base de los recursos que se van a tener en cuenta para así poder estudiar y desarrollar el proyecto.

## 1.4. ALCANCE Y LIMITACIONES DEL PROYECTO

Las redes de telecomunicaciones son esenciales en el funcionamiento organizacional de cualquier centro de trabajo hoy en día, todos los negocios buscan que su red de datos solucione las limitaciones de distancia y de tiempo cuando los proveedores y clientes de servicios se encuentran en distancias geográficas diferentes.

Por lo anterior, la principal importancia del documento, es presentar una propuesta de mejoramiento a la red de telecomunicaciones del cliente siguiendo las recomendaciones que sugiere Cisco System en su curso de certificación CCNP utilizando los equipos que existen actualmente, es decir, no se requieren nuevos equipos ni cableado.

A continuación se presentan los alcances y limitaciones del proyecto.

- Se realiza un análisis de la red actual del cliente para determinar los inconvenientes que este presenta para luego generar el plan de mejoramiento.
- Los problemas que se detecten en la red se basan en la teoría, en ningún momento se realizan mediciones de campo y tampoco se manipula físicamente los equipos del cliente.
- Con ayuda del simulador Cisco Packet Tracer se realizan los cambios necesarios para el mejoramiento de la red y se documentan en este proyecto.
- Los cambios y configuraciones necesarias para mejorar la red de cliente se basan en los fundamentos teóricos que presenta Cisco System en su curso de certificación CCNP para el diseño de redes.
- El simulador utilizado no permite emular los servicios del escenario real por lo que se presume que los problemas encontrados en la red son verídicos, basados en las prácticas y experiencias que ha comprobado Cisco System en sus investigaciones.
- La distancia entre las sedes no fue tenida en cuenta debido a que el transporte de datos a través de estas se realizaba por medio de otro operador local mediante una tecnología distinta.

Por temas de seguridad y confidencialidad, en el documento se denominará a la empresa como “cliente de telecomunicaciones”, el cual se encuentra ubicado en la ciudad de Bogotá. D.C. A su vez también se censura parte de la información presentada correspondiente a configuración y topología, la cual no es considerada relevante para realizar la propuesta.

## 1.5. METODOLOGÍA

En la elaboración del documento se utiliza un enfoque teórico basado en las recomendaciones de Cisco System para la configuración y diseño de redes de telecomunicaciones.

El proyecto se realizó una vez se finalizaron los módulos de certificación de *Routing* y *Switching* del curso CCNP, los cuales fueron necesarios para comprender y elaborar el plan de mejoramiento de la red de datos de un cliente de Telecomunicaciones.

Se procedió a estudiar la red actual del cliente y de esta manera comprender las configuraciones y los componentes presentes para luego generar un diagnóstico inicial sobre los problemas que se encuentran la red. Con la ayuda del simulador Cisco Packet Tracer se hace una simulación lo más cercana posible y se realizan las mejoras correspondientes.

Para la realización de este proyecto se utiliza la siguiente herramienta:

- Cisco Packet Tracer Windows Desktop Version 7.0 (64 bits).

Toda la información del documento se basa en la teoría y el material visto en los módulos de certificación de Cisco CCNP de *Routing* y *Switching*.

- CCNP R&S ROUTE: Implementing IP Routing 300-101 Certification Exam.
- CCNP R&S SWITCH: Implementing Ip *Switching* 300-115 Certification Exam.

El concepto de mejoramiento del rendimiento de una red se aborda desde el punto de vista de Cisco System en donde se define la gestión del rendimiento como:

"*La práctica de gestionar el tiempo de respuesta de los servicios de red, la coherencia y la calidad de los servicios individuales y globales. Los problemas de rendimiento suelen estar relacionados con la capacidad y rendimiento. Las aplicaciones son más lentas porque el ancho de banda y los datos deben esperar en las colas antes de ser transmitidos a través de la red. En aplicaciones como las de voz, existen problemas como el retardo y el jitter que afectan directamente a la calidad de la llamada de voz debido a la mala configuración y distribución de los servicios*." [6]*Traducido del Inglés.

# PARTE II

# FUNDAMENTOS TEÓRICOS

# **CAPÍTULO 2**
# FUNDAMENTOS TEÓRICOS

*En el siguiente capítulo se exponen todos los fundamentos teóricos que se deben tener en cuenta para entender la topología y los componentes de la red de telecomunicaciones y las diferentes tecnologías que la componen para proceder a generar una propuesta de mejoramiento.*

## 2.1. VIRTUAL LOCAL AREA NETWORK (VLAN)

Conocer la función de las VLAN y los enlaces troncales y cómo configurarlos hace parte de los conocimientos básicos necesarios para la construcción de una red. Las VLAN pueden extenderse a lo largo de toda la red o se pueden configurar para permanecer de manera local. Las VLAN juegan un papel crítico en el despliegue de las redes, incluso si no se es un especialista en uno de estos campos, es importante entender lo básico.

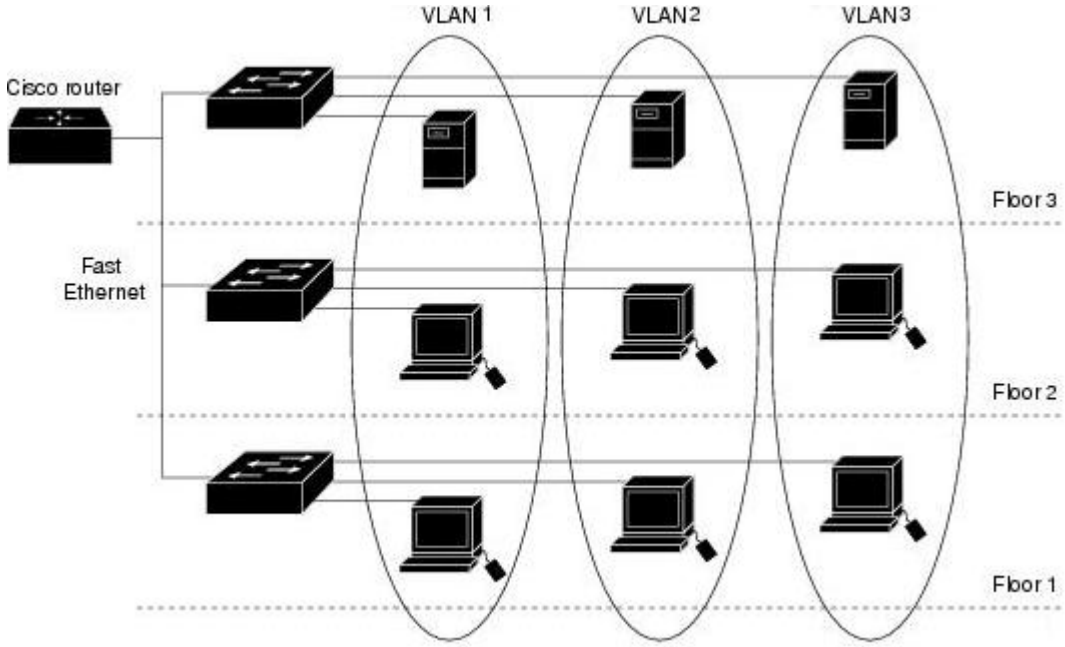



**Figura 1. Virtual local area network**
**Fuente:** http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/VLANs.html

Una VLAN es un grupo de estaciones finales con un conjunto común de requisitos, independientemente de su ubicación física, tiene los mismos atributos que una LAN física, excepto que le permite agrupar equipos finales, incluso cuando no se encuentran físicamente en el mismo segmento de LAN. Una VLAN también le permite agrupar puertos en un switch para que pueda limitar el tráfico *unicast*, *multicast*, y las inundaciones tráfico de difusión. Las inundaciones de tráfico que se originan a partir de una determinada VLAN solo fluyen a los puertos que pertenecen a esa VLAN.

Al crear VLAN, sus nombres y características se almacenan en la base de datos de VLAN. Hay un mecanismo llamado VTP (VLAN Trunking Protocol) que distribuye dinámicamente esta información entre switches. Sin embargo, incluso si no se va a utilizar en la red, se debería tener en cuenta, ya que puede causar estragos en algunas circunstancias.

Dentro de la interconexión de redes de conmutación, las VLAN proporcionan la segmentación y la flexibilidad para la organización, se puede diseñar una estructura de VLAN que permita grupos que están segmentados lógicamente por funciones, equipos y aplicaciones, sin tener en cuenta la ubicación física de los usuarios. Las VLAN permiten implementar políticas de acceso y de seguridad para determinados grupos de usuarios.

Existen varias funciones de VLAN, por ejemplo, La función VLAN de voz permite a los puertos de acceso llevar tráfico IP de voz a un teléfono IP, debido a que la calidad de sonido de una llamada de teléfono IP puede deteriorarse si los datos se envían de forma desigual y se configura QoS a una VLAN determinada.

### 2.1.1. Instrucciones del modo switchport

Los puertos de un switch de Cisco pueden ejecutar DTP (Dynamic Trunk Protocol), que puede negociar automáticamente un enlace troncal. Este protocolo propietario de Cisco System puede determinar un modo de enlace operativo y el protocolo en un puerto del switch cuando está conectado a otro dispositivo que también es capaz de negociar dinámicamente un enlace troncal.

| | DYNAMIC AUTO | DYNAMIC DESIRABLE | TRONCAL | ACCESO |
|---|---|---|---|---|
| DYNAMIC AUTO | Acceso | Troncal | Troncal | Acceso |
| DYNAMIC DESIRABLE | Troncal | Troncal | Troncal | Acceso |
| TRONCAL | Troncal | Troncal | Troncal | Conectividad Limitada |
| ACCESO | Acceso | Acceso | Conectividad Limitada | Acceso |

**Tabla 1. Instrucciones del Modo Switchport.**
**Fuente:** CCNP R&S SWITCHING: Implementing IP Switching 300-115 Certification Exam.

El modo de DTP predeterminado depende de la versión del software Cisco IOS y la plataforma. Para determinar el modo actual de VTP, se utiliza el comando **show interface** *slot/número*.

### 2.1.2. Implementación de las vlan

Se puede diseñar una red de campus empresarial con dos tipos diferentes de implementaciones VLAN: end-to-end (extremo a extremo) o locales; cada modelo posee sus ventajas y sus desventajas.

El término end-to-end VLAN se refiere a una única VLAN que está asociada con los puertos de conmutación que están dispersos en una red empresarial en múltiples switches. Una red conmutada de capa 2 transporta esta VLAN en toda la red.

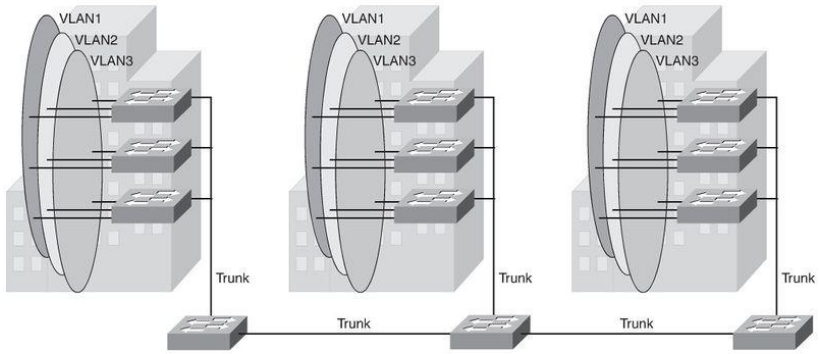



**Figura 2. End-to-end VLAN.**
**Fuente:** http://ciscodocuments.blogspot.com.co/2011/05/chapter-02-implementing-VLANs-in-campus.html

Un modelo de VLAN de extremo a extremo tiene estas características:

- Cada VLAN es transportada geográficamente a través de la red.
- Los usuarios son agrupados en la VLAN sin importar su ubicación física.
- A medida que un usuario se mueve a lo largo de una red, el usuario se moverá a través de la misma VLAN, independientemente del *switch* al que este usuario se conecta.
- Los usuarios son típicamente asociados con una VLAN determinada por razones de gestión de red. Esta razón es por lo que se mantienen en la misma VLAN, y por lo tanto en el mismo grupo, mientras que se mueven a través de la red.
- Todos los dispositivos en una VLAN determinada suelen tener direcciones en la misma subred.

La arquitectura de campus de Cisco System se basa en el modelo de VLAN local. En este modelo de VLAN, todos los usuarios de un conjunto de switches geográficamente comunes se agrupan en una sola VLAN, independientemente de la función de la organización de estos usuarios. Si los usuarios se mueven de un lugar a otro en el campus, su conexión se cambia a la nueva VLAN en la nueva ubicación física.

En el modelo local de VLAN, la capa 2 de conmutación se utiliza en nivel de acceso, y el enrutamiento se utiliza en los niveles de distribución y de core para permitir a los usuarios mantener el acceso a los recursos que necesitan.

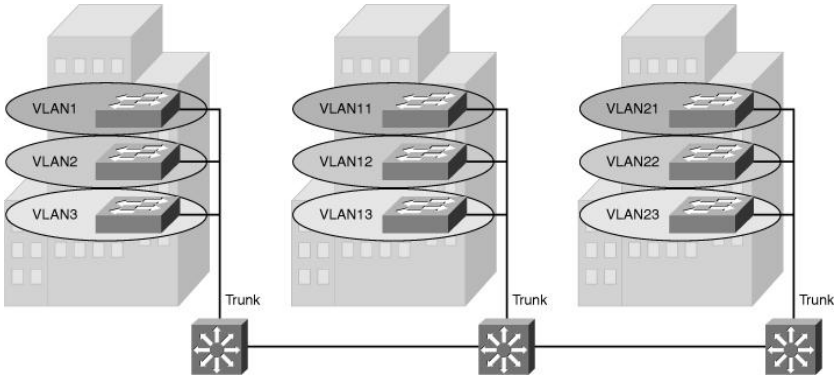



**Figura 3. Local VLAN.**

**Fuente:** http://ciscodocuments.blogspot.com.co/2011/05/chapter-02-implementing-VLANs-in-campus.html

A continuación algunas características de este modelo.

- El tráfico de VLAN local es sobre la capa 2 de conmutación entre los niveles de acceso y distribución.
- El tráfico de VLAN local se enruta a nivel de distribución y core para llegar a destinos en otras redes.
- Una red que consta en su totalidad de VLAN locales pueden beneficiarse con mayores tiempos de convergencia que se ofrecen a través de los protocolos de enrutamiento, en lugar de STP para redes de capa 2.

### 2.1.3. VLAN extremo a extremo vs VLAN locales

En el pasado, los diseñadores de redes han tratado de poner en práctica la regla 80-20 en el diseño de redes. La regla se basa en la observación de que, en general, se pasó a 80 por ciento del tráfico en un segmentos de red entre dispositivos locales, y sólo el 20 por ciento del tráfico estaba destinado a segmentos de red remota, por lo tanto, se utilizaban normalmente las VLAN de extremo a extremo. Los diseñadores ahora consolidan los servidores en lugares centrales en la red y proporcionan acceso a los recursos externos, tales como el Internet a través de una o dos rutas en la red debido a que la mayor parte del tráfico atraviesa ahora una serie de segmentos. Por lo tanto, el paradigma ahora está más cerca de 20 a 80 de la porción, en la cual el mayor flujo de tráfico que sale del segmento local por lo que las VLAN locales se han vuelto más eficiente.

| VLAN Extremo a Extremo | VLAN Locales |
|---|---|
| **Pros:**<br>• Usuarios geográficamente dispersos en el mismo segmento.<br>• la misma política (seguridad, QoS) se puede aplicar al mismo grupo de usuarios, independientemente de su ubicación física. | **Pros:**<br>• El diseño es escalable.<br>• La resolución de problemas es fácil.<br>• El flujo de tráfico es predecible.<br>• Las rutas redundantes se pueden construir fácilmente. |
| **Cons:**<br>• Todos los switches tienen que saber todas las VLAN.<br>• Los mensajes de difusión inundan todos los switches.<br>• La solución de problemas puede ser un reto. | **Cons:**<br>• Se requieren más dispositivos de enrutamiento que en los modelos de extremo a extremo.<br>• Los usuarios pertenecen al mismo dominio de difusión cuando están en la misma ubicación. |

**Tabla 2. End-to-end VLAN vs Local VLAN.**
**Fuente:** CCNP R&S SWITCHING: Implementing IP Switching 300-115 Certification Exam.

Debido a que las VLAN representan un segmento de la capa 3, cada VLAN de extremo a extremo permite que un solo segmento de la capa 3 que se disperse geográficamente por toda la red. La implementación de este diseño puede ser implementado por las siguientes razones:

- Agrupación de servidores: Los usuarios se pueden agrupar en un segmento IP común, a pesar de que están dispersos geográficamente.
- Seguridad: una VLAN puede contener recursos que no deben ser accesible a todos los usuarios de la red, o puede haber razón para limitar la circulación de determinadas VLAN en particular.
- Aplicación de QoS: todo el tráfico de una determinada VLAN se le puede dar una prioridad de acceso más alta o más baja a los recursos de la red.
- Evitar enrutamiento: si la mayor parte del tráfico de los usuarios de la VLAN está destinado a dispositivos en la misma VLAN y enrutamiento para esos dispositivos no es deseable, los usuarios pueden acceder a los recursos de la VLAN sin enrutar el trafico fuera de la VLAN, incluso si el tráfico puede atravesar múltiples switches.
- VLAN de propósito especial: a veces una VLAN se configura para llevar a un solo tipo de tráfico que debe ser dispersado por toda la red (por ejemplo, *multicast*, voz)

Estos son algunos elementos que se deben considerar en la aplicación de las VLAN de extremo a extremo:

- Los puertos de conmutación se aprovisionan para cada usuario y se asocian con una VLAN dada; debido a que los usuarios de una VLAN de extremo a extremo pueden estar en cualquier lugar en la red, todos los switches deben estar al tanto y conocer tal VLAN. Esto significa que se requiere que todos los switches que transportan tráfico de VLAN de extremo a extremo deben tener esas VLAN específicas definidas en la base de datos de la VLAN de cada switch.
- La inundación de tráfico para las VLAN es por defecto, pasa a todos los switches incluso si no tienen ninguno de los puertos activos.
- La solución de problemas (*Troubleshooting*) en un campus de red con VLAN de extremo a extremo puede ser un reto debido a que el tráfico de una sola VLAN puede atravesar varios switches en una amplia zona del campus.

El concepto de VLAN de extremo a extremo era muy atractivo cuando la configuración de direccionamiento IP se administraba de forma manual, lo cual era un proceso tedioso; por lo tanto, cualquier cosa que redujera el trabajo, era una mejora a causa de los usuarios que se mueven constantemente entre redes. Por esta razón, la ubicuidad de DHCP hace que el proceso de configuración de una dirección IP a cada puesto de trabajo ya no sea un problema importante. Como resultado, hay pocos beneficios para la extensión de una VLAN en toda la empresa.

Las VLAN locales son parte del diseño de la arquitectura campus de empresa de Cisco System, en la que las VLAN que se utilizan en la capa de acceso deben extenderse solo con su asociado de distribución. El tráfico se encamina desde la VLAN local, ya que se pasa de la capa de distribución al núcleo. Este diseño puede mitigar los problemas de la capa 2 para la solución de problemas que se producen cuando una sola VLAN atraviesa los switches en la red de campus de la empresa. La implementación del diseño de la arquitectura campus de empresa utilizando las VLAN locales ofrece estos beneficios:

- **El flujo de tráfico determinista:** Un diseño simple proporciona una trayectoria predecible en el tráfico de Capa 2 y Capa 3. En el caso de un fallo que no fue mitigado por las características de redundancia, la simplicidad del modelo facilita el aislamiento de problemas y la resolución dentro del bloque de switches.

- **Ruta activa redundante:** Al aplicar TSVP (Resource Reservation Protocol) o MST (Multi Spanning Tree Protocol), se pueden utilizar todos los enlaces para hacer uso de las rutas redundantes.

- **Alta disponibilidad:** Existen rutas redundantes en todos los niveles de infraestructura. El tráfico de VLAN local en los switches de acceso se puede pasar a los switches de distribución del edificio a través de una vía alternativa de capa 2 en caso de algún fallo de la ruta primaria. Los protocolos de redundancia en los routers proveen conmutación en caso error en caso de que la puerta de enlace predeterminada para la VLAN de acceso falle. Cuando STP y las VLAN están confinados a un bloque de acceso y distribución específica, los protocolos de redundancia de las capas 2 y 3 deben ser configurados para la conmutación de manera coordinada.

- **Dominio de error finito:** Si la VLAN local de un bloque de switches, y el número de dispositivos en cada VLAN se mantiene pequeño, los fallos en la capa 2 se limitan a un pequeño subconjunto de usuarios.

- **Diseño escalable:** Siguiendo el diseño de la arquitectura campus de empresa, se pueden incorporar fácilmente nuevos switches de acceso, y añadir nuevos submódulos cuando sea necesario.

### 2.1.4. VLAN trunking protocol (VTP)

VTP es un protocolo propietario de Cisco System que gestiona las VLAN. Cuando se configura una nueva VLAN en un servidor VTP, La VLAN se distribuye a través de todos los switches en el dominio. Si se usa con cuidado, VTP puede reducir la necesidad de configurar la misma VLAN en todas partes, sin embargo, si no es consciente de todas las advertencias, puede causar estragos en la red.

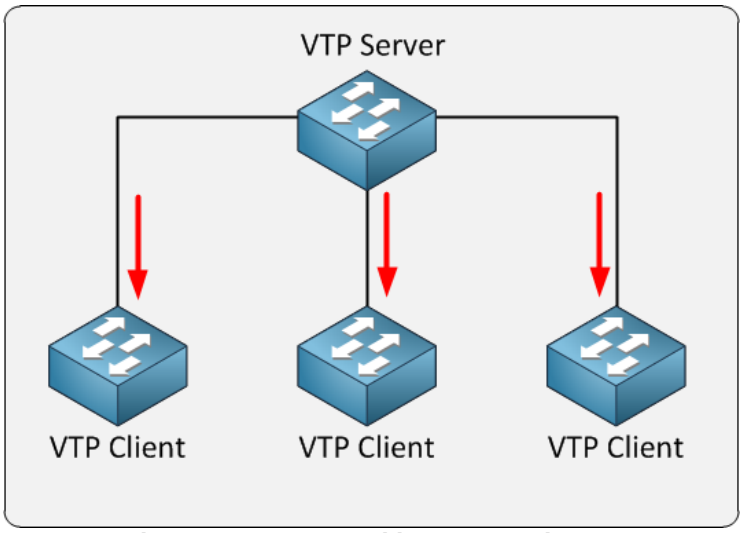



**Figura 4. VLAN Trunking Protocol.**
**Fuente:** http://www.giantsnet.com/2014/03/vtp-VLAN-trunk-protocol.html

VTP es un protocolo de capa 2 que mantiene la consistencia de la configuración de las VLAN mediante la gestión de las adiciones, eliminaciones y cambios de nombres de VLAN a través de la red.

Un dominio de VTP es un switch o varios switches interconectados que comparten el mismo entorno de VTP, incluso se puede configurar un switch para estar en un solo dominio VTP. Por defecto, un switch Cisco Catalyst está en el estado de “no-management-domain” o "<null>" hasta que se recibe y anuncio de un dominio a través de un enlace troncal o hasta que configure un dominio de gestión. Las configuraciones que se realizan en un único servidor VTP se propagan a través de enlaces troncales para todos los switches conectados en la red y las configuraciones cambiarán si el dominio VTP y las contraseñas de VTP coinciden.

### 2.1.5. Modos de VTP

VTP opera en uno de sus tres modos: Servidor, Transparente o Cliente. En algunos switches, VTP puede estar incluso deshabilitado.

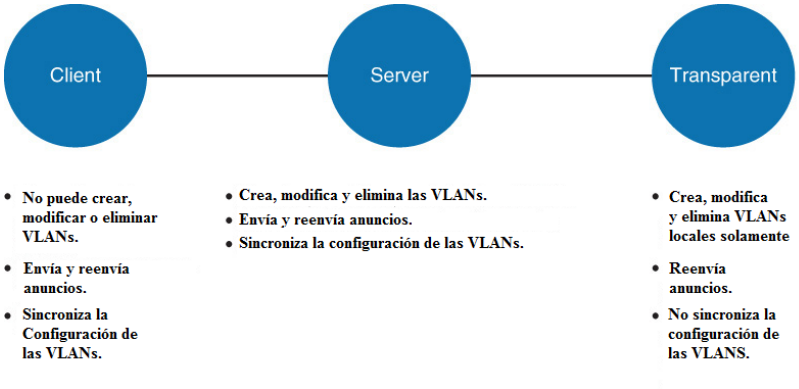



**Figura 5. Modos de VTP.**
**Fuente:** http://www.ciscopress.com/articles/article.asp?p=2348266&seqNum=2

Las características de los tres modos de VTP son los siguientes:

- **Servidor:** el modo VTP predeterminado es el modo de servidor, las VLAN no se propagan por la red hasta que se especifique o se aprenda un nombre de dominio de gestión. Cuando se realiza un cambio en la configuración de una VLAN en el servidor VTP, el cambio se propaga a todos los switches en el dominio de VTP. Los mensajes VTP se transmiten a todos los puertos troncales.
- **Transparente:** Cuando se realiza un cambio en la configuración de VLAN en el modo VTP transparente, el cambio sólo afecta al switch local. El cambio no se propaga a otros switches en el dominio VTP. el modo VTP transparente no remite publicaciones VTP que recibe dentro del dominio.
- **Cliente:** Un cliente del VTP se comporta como un servidor VTP, transmite y recibe actualizaciones VTP en sus puertos troncales pero no puede crear, modificar o borrar las VLAN en un cliente de VTP. Las VLAN se configuran en otro switch que esté en el dominio y se encuentre en modo servidor.

En los modos de servidor, transparente y cliente, las publicaciones VTP se reciben y se transmiten tan pronto como el switch entra en el estado de dominio de gestión. En el modo “Off” los switches se comportan de la misma manera que en el modo VTP transparente, con la excepción de que los avisos de VTP no se reenvían. El modo “Off” no está disponible en todas las versiones.

Los servidores y clientes VTP de Cisco Internetwork guardan las VLAN en el archivo VLAN.dat en la memoria flash, lo que les permite mantener la tabla de VLAN y el número de revisión. Los switches que están en modo VTP transparente visualizan la VLAN y configuraciones VTP con el comando **show running-config** ya que esta información se almacena en el archivo de texto de configuración. Si se realiza **erase startup-config** en un switch VTP transparente, eliminará sus VLAN.

## 2.2. DISEÑO DE REDES.

El Campus Empresarial es la parte de la infraestructura de la red que proporciona acceso a los servicios y recursos de comunicaciones de los dispositivos que estén situados en una ubicación geográfica particular; este campus puede abarcar una planta, un edificio o incluso un grupo grande de edificios que se extienden sobre un área geográfica más amplia.

El diseño de una red de campus no es diferente a cualquier otro sistema, el uso de una guía fundamental de principios fundamentales de Networking serviría para asegurar el diseño que el campus ofrece en cuanto a disponibilidad, seguridad, flexibilidad y manejabilidad los cuales son requisitos para satisfacer las necesidades actuales de negocio y tecnológicas futuras.

### 2.2.1. Diseño jerárquico de una red

El Campus Empresarial plano es la parte en donde todos los PCs, servidores, impresoras, entre otros dispositivos se conectan entre sí mediante switches capa 2. Una red plana no tiene subredes, todos los dispositivos en esta subred comparten el ancho de banda disponible y son miembros del mismo dominio de difusión. Un paquete de difusión utiliza tiempo de CPU en cada dispositivo dentro del dominio de difusión. Una red de 10 dispositivos en el mismo segmento no debería causar problemas, pero si en vez de 10 son cientos en la misma subred, es muy seguro que la red comience a presentar problemas y de seguro no funcionará bien.

El uso de dispositivos capa 3, como un router o un switch multicapa es esencial para segmentar una red, ya que los paquetes que se originan dentro de una subred no se propagarán más allá del borde del segmento de LAN.
Existen 3 componentes que pueden ayudar a saber si existe un buen diseño de red.

- Si se puede duplicar el tamaño de la red sin mayores cambios en el diseño.
- Si se puede agregar componentes a la red solo con hacer cambios a los dispositivos directamente conectados.
- Si se sabe cómo añadir un nuevo enlace WAN, piso edificios, rama, etc.

### 2.2.2. Capas en el modelo jerárquico

Los modelos jerárquicos para el diseño e interconexión de redes permiten diseñar redes en capa. Para comprender la importancia del modelo de capas hay que tener en cuenta el modelo de referencia OSI, el cual es un modelo de capas para comprender e implementar comunicaciones informáticas. Mediante el uso de capas del modelo OSI se simplifica la tarea que se requiere para que dos ordenadores se comuniquen. El modelo de arquitectura empresarial de Cisco System también utiliza capas para simplificar la tarea que se requiere para la interconexión de redes

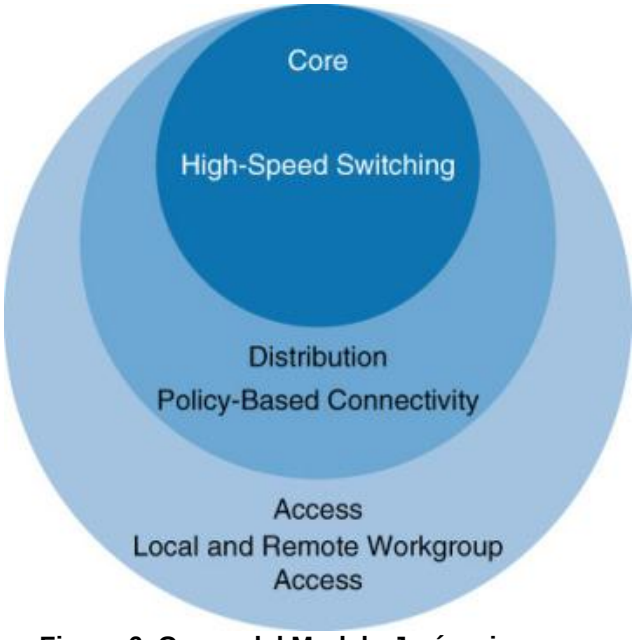



**Figura 6. Capas del Modelo Jerárquico.**
**Fuente:** http://www.ciscopress.com/articles/article.asp?p=2348265

Cada capa se centra en funciones específicas, lo que le permite elegir el sistema adecuado y las características de la capa. Este modelo proporciona un marco modular que permite flexibilidad en el diseño de la red y facilita la aplicación y resolución de problemas. El campus de la empresa divide sus redes o bloques modulares en Acceso, Distribución y Núcleo con las siguientes características: (Access, Distribution, Core.).

- ***Capa de Acceso:*** La capa de acceso se utiliza para conceder acceso de usuarios a los dispositivos de red. En un campus de la red, la capa de acceso generalmente incorporan switchs de los dispositivos de LAN con puertos que permite la conectividad con las estaciones de trabajo y los servidores. En el entorno WAN, la capa de acceso para los trabajadores a distancia o en los sitios remotos puede proporcionar acceso a la red corporativa a través de la tecnología WAN.

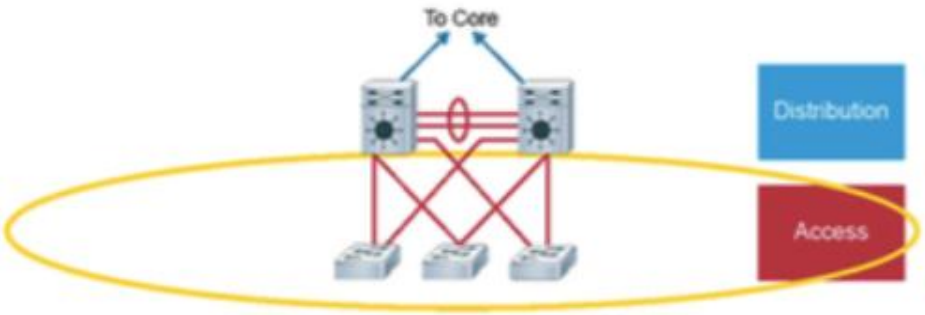



**Figura 7. Capa de Acceso.**
**Fuente:** CCNP R&S SWITCHING: Implementing IP Switching 300-115 Certification Exam.

La capa de acceso es el lugar donde los dispositivos finales (PCs, impresoras, cámaras y similares) se unen a la red cableada del campus. También es el lugar en donde son conectados los dispositivos que extienden la red un nivel más tales como teléfonos IP, Puntos de acceso, y Wireless. La amplia variedad de dispositivos que se pueden conectar, los diferentes servicios y los mecanismos de configuración dinámicos que son necesarios, hacen que la capa de acceso sea la más destaca de la red y poseen las siguientes características:

*Alta disponibilidad:* la capa de acceso está conformada por mucho Hardware y Software. Ofrece acceso redundante al Gateway predeterminado utilizando dos conexiones de los switches de acceso a los switches de distribución utilizando FHRP.

*Convergencia*: la capa de acceso es compatible con PoE para telefonía IP y Access Points inalámbricos, permitiendo a los clientes converger con voz en su red de datos.

*Seguridad*: la capa de acceso proporciona servicios de seguridad adicional contra el acceso no autorizado a la red mediante el uso de herramientas como DHCPsnooping, DAI, IP Source Guard, seguridad a los puertos.

- ***Capa de Distribución:*** La capa de distribución agrega el cableado, utilizando switches para segmentar los grupos de trabajo y aislar los problemas en el entorno de red. Así mismo también agrega las conexiones WAN en el borde y proporciona conectividad basada en políticas.

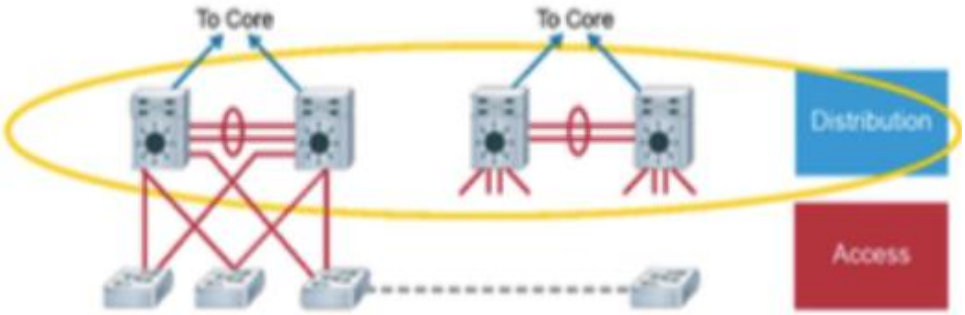



**Figura 8. Capa de Distribución.**
**Fuente:** CCNP R&S SWITCHING: Implementing IP Switching 300-115 Certification Exam.

En el diseño de red, la capa de distribución tiene un papel único en la que actúa como un límite de servicios y de control entre la capa de acceso y el núcleo, tanto la capa de núcleo y acceso son capas de propósito especial, la capa de acceso está dedicado a satisfacer las funciones de conectividad de los dispositivos finales y la capa de core se dedica a proporcionar conectividad sin parar a través de toda la red. La capa de distribución por otra parte, es multipropósito.

La disponibilidad, la recuperación del camino, balance de carga y la calidad de servicio son las consideraciones importantes en la capa de distribución. La disponibilidad es comúnmente proporcionada gracias a la redundancia de los enlaces hacia el core y de la capa de acceso a la de distribución. Una distribución de igual costo en enlaces de capa 3 permite que ambos enlaces ascendentes de la capa de distribución sean utilizados.

La capa de distribución en el lugar en donde se lleva a cabo el enrutamiento y la manipulación de paquetes actuando como frontera entre la capa de acceso y núcleo. La capa de distribución lleva a cabo tareas tales como control del protocolo de enrutamiento y resume (summary) las rutas que forman parte de la capa de acceso; para algunas redes ofrece una ruta por defecto a los switches de acceso y ejecuta protocolos de enrutamiento dinámico contra el núcleo.

La capa de distribución utiliza una combinación de capa 2 y conmutación multicapa para segmentar las estaciones de trabajo y aislar problemas de red para que no afecten el núcleo. Por lo general es usada para aislar las VLAN

de acceso, y generar políticas de QoS, seguridad, carga de tráfico y enrutamiento. Proporciona redundancia de Gateway predeterminado utilizando protocolos como HSRP, FHRP, VRRP o GLPB. FHRP permite la insuficiencia o la eliminación de uno de los nodos de distribución sin afectar la conectividad del Gateway.

- ***Capa de Core:*** También llamado "*Backbone*", es la cadena principal de alta velocidad que está diseñada para conmutar paquetes tan rápido como sea posible. Debido a que es fundamental para la conectividad, debe poseer un alto grado de disponibilidad y adaptarse a los cambios muy rápidamente; también proporciona escalabilidad y un alto grado de convergencia.

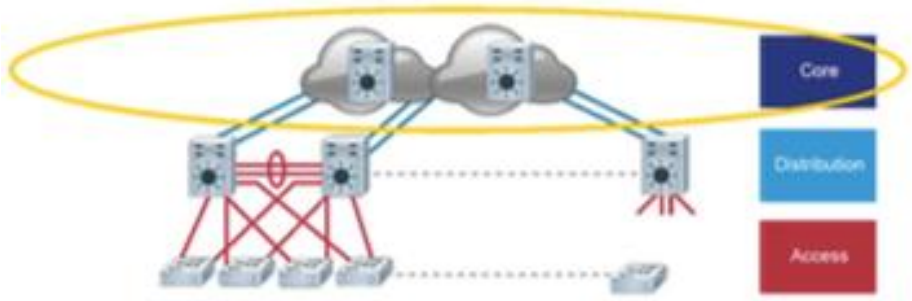



**Figura 9. Capa de Core.**
**Fuente:** CCNP R&S SWITCHING: Implementing IP Switching 300-115 Certification Exam.

El core de la red es, en algunos aspectos, la parte más importante y simple de la red. Proporciona un conjunto muy limitado de servicios y está diseñado para tener una muy alta disponibilidad y operar en modo activo. En el mundo de los negocios modernos, el core de la red debe funcionar como un servicio sin escalas, los parámetros de diseños claves para el core deben proporcionar un nivel de redundancia adecuada para permitir la recuperación del flujo de datos los más rápido e inmediato posible en caso de que falle cualquier componente (switch, supervisor, tarjeta de línea o fibra). El diseño de la red deberá permitir en ocasiones la actualización de la red sin interrumpir ningún proceso que se esté llevando a cabo. El core de la red no debe implementar ninguna política de servicio y no debe tener ningún usuario o servidor conectado directamente.

El core es la cadena principal que une todos los elementos de la arquitectura de red. Es la parte de la red que proporciona la conectividad entre los dispositivos finales, cómputo y servicios de almacenamiento de datos que se encuentran dentro del centro de datos - y otras áreas y servicios dentro de la red.

En entornos en los que la red está contenida en un solo edificio o varios edificios adyacentes, con la cantidad adecuada enlaces es posible prescindir de los conmutadores de núcleo y conectar directamente los switches de distribución.

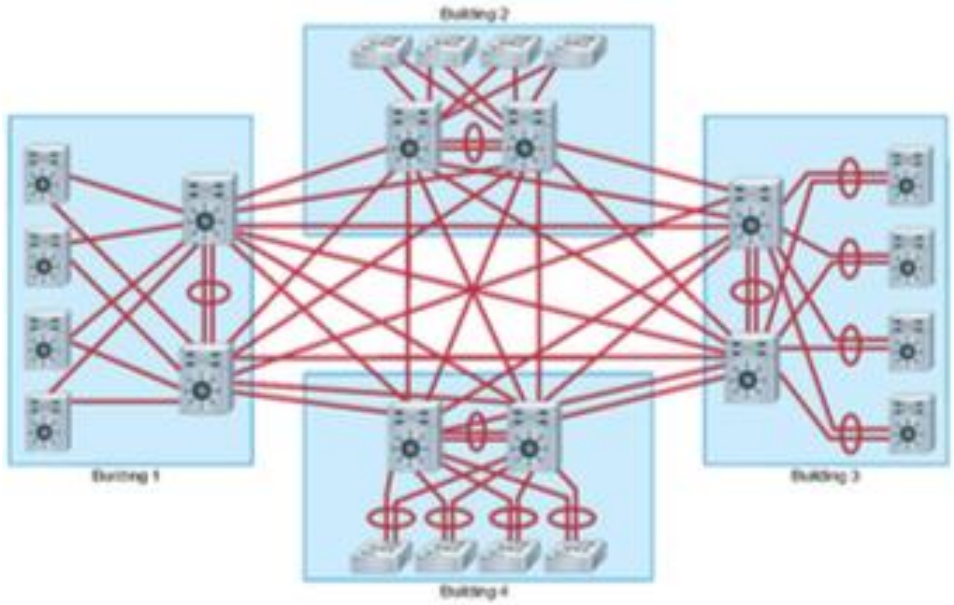


**Figura 10. Red Sin Capa de Core.**
**Fuente:** CCNP R&S SWITCHING: Implementing IP Switching 300-115 Certification Exam.

Sin una capa de núcleo, se tendrá una malla en los enlaces entre los switches de la capa de distribución. Este diseño es difícil de escalar, y aumenta los requisitos de cableado, ya que cada nuevo interruptor de distribución del edificio necesita conectividad completa para todos los switches de distribución. La complejidad de enlaces en el diseño aumenta a medida que añada nuevos vecinos y multiplicara los enlaces.

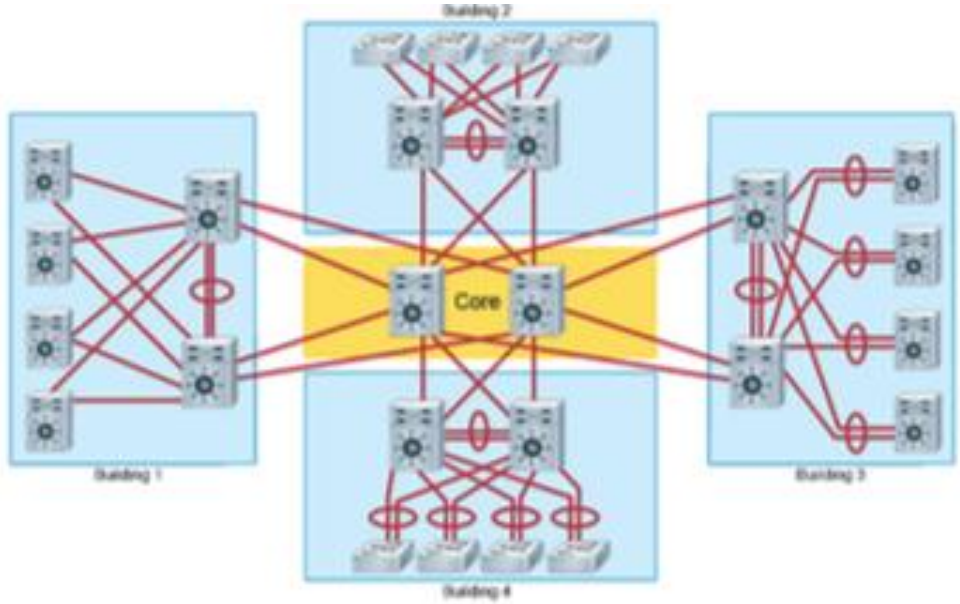



**Figura 11. Red Con Capa de Core.**
**Fuente:** CCNP R&S SWITCHING: Implementing IP Switching 300-115 Certification Exam.

Tener una capa de core permite a la red crecer sin comprometer el diseño de los bloques de distribución, el data center, y el resto de la red. Esto es particularmente importante ya que el tamaño de la red depende tanto del número de bloques de distribución el área geográfica y la complejidad. En un campus más grande y más complejo, el núcleo proporciona la capacidad de escalamiento en todo el diseño de la red.

Cuándo es necesario un core dentro de la red dependerá de múltiples factores. La capacidad de un core para permitir resolver los retos de diseño físico es importante, sin embargo, debe recordarse que el propósito central de contar con un core es proporcionar escalabilidad y reducir al mínimo el riesgo (y simplificar) movimientos, adiciones y cambios dentro de la red.

En la figura 11 se ve cómo se reduce el número de enlaces con respecto a cuándo la capa de distribución funciona como núcleo, permitiendo que se puedan agregar nuevos switches de distribución agregando un par de conexiones nuevas.

## 2.3 SPANNING TREE PROTOCOL (STP).

STP permite utilizar topologías redundantes, evitando bucles de Capa 2. Por defecto los switches Cisco utilizan TSVP+ (Resource Reservation Protocol+). Sin embargo, siempre que sea posible, se debe utilizar ya sea Rapid PVST+ o MSTP (MultiSTP). STP provee diferentes configuraciones, algunas se implementan para acelerar el rendimiento (UplinkFast BackboneFast, PortFast), y otros están configurados para aumentar la estabilidad (BPDU guard, BPDU filter, root guard, loop guard). También existen otros mecanismos que no están directamente relacionados con STP, pero se pueden utilizar para complementar el funcionamiento de STP (UDLD) o reemplazarlo por (FlexLinks).

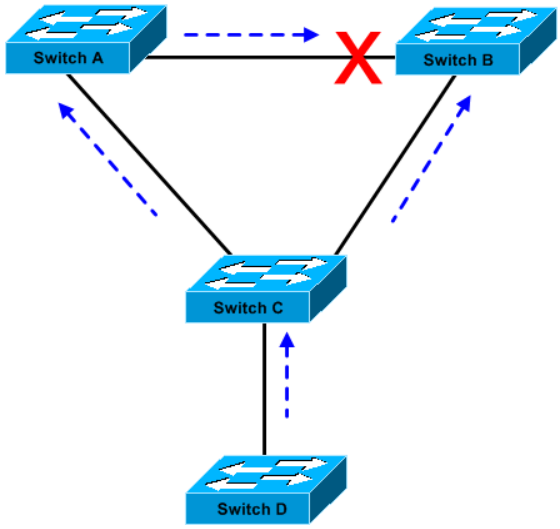



**Figura 12. Spanning Tree Protocol.**
**Fuente:** http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10586-65.html.

Una topología redundante puede evitar que un fallo en un único enlace de la red cause perdidas en toda la topología. Por otro lado, usar una topología redundante puede causar diferentes problemas como.

- **Tormentas de *Broadcast*:** Cada switch en una red redundante envía tramas de difusión sin fin, estos envían tramas de *broadcast* a todos los puertos excepto en el cual la trama fue recibida, formando un bucle en todas las direcciones.

- **Transmisión de Múltiples Tramas (Multiple Frame Transmission):** Múltiples copias de la misma trama de *unicast* pueden ser entregados a una red de destino, lo cual puede causar problemas con el protocolo de recepción. muchos protocolos esperan recibir una sola copia de cada transmisión por lo que múltiples copias de la misma trama puede producir errores irrecuperables.

- **Inestabilidad de la base de datos MAC (MAC Database Instability):** Este problema se produce cuando muchas copias de la misma trama están siendo recibidas por diferentes puertos en el switch. La tabla de direcciones MAC asigna la dirección MAC de origen en un paquete de recibido en la interfaz que se recibió. Si se produce un bucle, la misma dirección MAC de origen podría ser vista en múltiples interfaces, causando inestabilidad. el reenvío de datos puede verse afectado porque el switch consume muchos de sus recursos intentando resolver a la inestabilidad en la tabla de direcciones MAC.

Para resolver todos estos problemas, es necesario un mecanismo para evitar bucles. STP fue desarrollado para abordar estas cuestiones, permite la redundancia al tiempo que evita los efectos indeseables de los bucles activos en la red. STP obliga determinado puerto a ponerse en estado de espera a fin de que no escuche o reenvié tramas de datos que inunden la red causando que sólo haya una ruta activa a cada segmento de red.

Si hay un problema con la conectividad a cualquiera de los segmentos, STP restablece la conectividad activando automáticamente una trayectoria previamente inactiva. Los BPDU son mensajes que STP utiliza para determinar la información de topología actual, de forma predeterminada, se envían a cabo cada 2 segundos en todos los puertos del switch.

### 2.3.1. Estándares de STP

| | Estándar | Utilización de Recursos | Convergencia | |
|---|---|---|---|---|
| **CST** | **802.1D** | **Bajo** | **Lento** | **Todas VLAN** |
| **PVST+** | **Cisco** | **Alto** | **Lento** | **Cada VLAN** |
| **RSTP** | **802.1w** | **Medio** | **Rápido** | **Todas VLAN** |
| **Rapid PVST+** | **Cisco** | **Muy alto** | **Rápido** | **Cada VLAN** |
| **MSTP** | **802.1s** | **Medio-Alto** | **Rápido** | **Lista VLAN** |

**Tabla 3. Estándares de STP.**
**Fuente:** CCNP R&S SWITCHING: Implementing IP Switching 300-115 Certification Exam.

- **STP:** Es la versión original IEE.802.1D que proporciona una topología libre de bucles en una red con enlaces redundantes. STP fue creado para redes “Bridges” o de capa 2 por lo que soportan una única red LAN o una VLAN.

- **CST:** Una instancia STP para toda la red. CST asume una instancia de spanning-tree para toda la red. A diferencia del 802.1D, soporta más de una VLAN.

- **PVST y PVST+:** Proporcionar una instancia de STP por separado para cada VLAN. PVST y PVST+ son propiedad de Cisco que proporcionan una instancia de spanning-tree independiente para cada VLAN configurada en la red. PVST quedó obsoleta con la aparición de PVST+

- **MSTP:** MST mapea múltiples VLAN en la misma instancia de spanning-tree.

- **RSTP:** Es un STP con una convergencia mucho más rápida. Su estándar está descrito en la IEE 802.1w. es la evolución de STP la cual proporciona mayor convergencia STP.

- **Rapid PVST+:** Es una implementación de Cisco para RSTP que proporciona una instancia de STP por separado para cada VLAN y es basado en PVST+.

### 2.3.2. Funcionamiento de STP

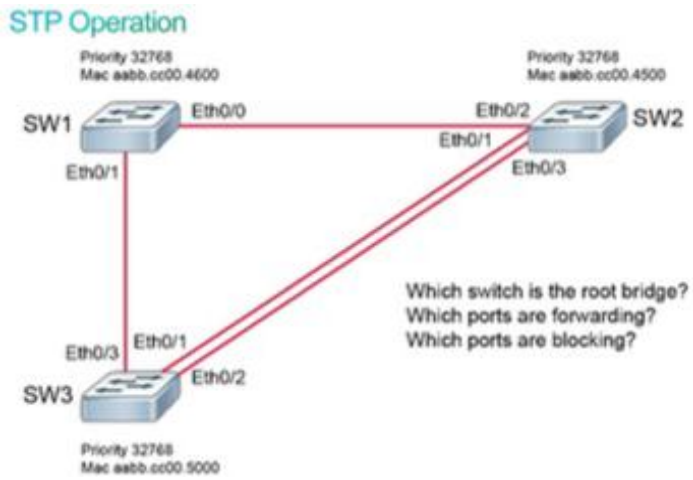



**Figura 13. Funcionamiento de STP.**
**Fuente:** CCNP R&S SWITCHING: Implementing IP Switching 300-115 Certification Exam.

STP proporciona una resolución mediante la gestión de una ruta física en un segmento de red determinado realizando tres pasos:

1. **Elige a un puente raíz:** Sólo un puente puede actuar como puente raíz. El puente raíz es el punto de referencia, y todo el flujo de datos de la red es desde la perspectiva del switch. Todos los puertos de un puente raíz están reenviando tráfico.

2. **Selecciona el puerto raíz en el puente no raíz:** Un puerto en cada puente no raíz es el puerto raíz. Es el puerto con la ruta de menor costo desde el puente no raíz al puente raíz. Por defecto, el coste de la ruta STP se calcula a partir del ancho de banda del enlace. También se puede establecer el coste de la ruta STP manualmente.

3. **Selecciona el puerto designado en cada segmento:** Hay un puerto designado en cada segmento. La selección se realiza en el puente con el camino de menor costo para el puente raíz.

Los puertos que no son ni raíz o designado deben ser no designados. Los puertos no designados están normalmente en estado de bloqueo para romper el bucle en la topología. Existen 4 perfiles en los puertos STP:

| Perfil del Puerto | Descripción |
|---|---|
| Root Port | Existe este puerto en los puentes que no son root y es el puerto del switch con la mejor ruta hacia el puente raíz. Sólo un puerto raíz está permitido por cada puente. |
| Designated Port | Un puerto designado es el puerto del switch que va a recibir y enviar hacia el puente raíz, según sea necesario. Sólo se permite un puerto designado por segmento. Si existen varios switches en el mismo segmento, un proceso de elección determina el switch designado, y el puerto del switch correspondiente comienza el reenvío de tramas para el segmento. |
| Nondesignated Port | El puerto no designado es un puerto del switch que no envía (por bloqueo) tramas de datos. |
| Disable Port | El puerto inhabilitado es el puerto del switch que está apagado. |

**Tabla 4. Perfil del Puerto STP.**
**Fuente:** CCNP R&S SWITCHING: Implementing IP Switching 300-115 Certification Exam.

Los puertos de un switch que tiene habilitado el protocolo STP se encuentran en los siguientes estados.

| Estado del puerto STP | Recibe BPDUs | Envía BPDUs | Aprende Direcciones MAC | Recibe Datos | Envía Datos | Duración del Estado |
|---|---|---|---|---|---|---|
| Blocking | √ | X | X | X | X | Indefinido (Si hay loop) |
| Listening | √ | √ | X | X | X | Retardo de envío (15 Segs) |
| Learning | √ | √ | √ | X | X | Retardo de envío (15 Segs) |
| Forwarding | √ | √ | √ | √ | √ | Indefinido (Tanto hasta cuando no halla loop) |
| Disabled | X | X | X | X | X | Hasta que el administrador lo habilite |

**Tabla 5. Estado del Puerto STP.**
**Fuente:** CCNP R&S SWITCHING: Implementing IP Switching 300-115 Certification Exam.

Un switch no entra en ninguno de estos estados de puerto inmediatamente excepto el estado de blocking. Cuando se habilita el protocolo Spanning Tree (STP), cada switch de la red comienza en el estado de blocking y más tarde cambia a los estados de listening y learning.

### 2.3.3. Herramientas STP de Cisco System

Las herramientas STP de cisco proporcionan unos mejor manejos de STP. Entre las que se destacan las siguientes.

- **UplinkFast**

Si falla el enlace de reenvío, se tardará entre 30 y 50 segundos para el otro enlace tome el relevo. UplinkFast es una solución propietaria de Cisco que reduce en gran medida el tiempo de convergencia.

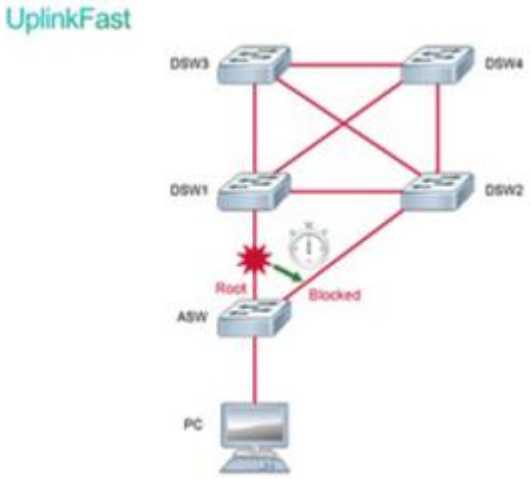



**Figura 14. UplinkFast.**
**Fuente:** CCNP R&S SWITCHING: Implementing IP Switching 300-115 Certification Exam.

La característica UplinkFast se basa en la definición de grupo de enlace ascendente. En un switch dado, el grupo de enlace ascendente consiste en el puerto raíz y todos los puertos que proporcionan una conexión alternativa al puente raíz. Si el puerto raíz falla, lo que significa un fallo en el enlace ascendente primario, el puerto de más bajo costo del grupo de enlaces ascendentes es seleccionado para la sustitución inmediatamente.

Para acelerar el tiempo de recuperación, el switch de capa de acceso comenzará a anunciar todas las direcciones MAC como direcciones de origen en tramas de multidifusión ficticias que se envían a través del nuevo puerto de reenvío. El tiempo total para recuperar el fallo de enlace primario será normalmente menos de un segundo.

En la figura, si el puerto raíz Ethernet 0/1 de ASW falla el puerto Ethernet 0/2 será inmediatamente el puerto activo si tiene UplinkFast activado.

UplinkFast solo funciona cuando el switch ha bloqueado los puertos. La función está diseñada típicamente para un switch de acceso que tiene enlaces ascendentes redundantes bloqueados. Cuando se habilita UplinkFast, se habilita para todo el switch y no se puede habilitar para las VLAN individuales.

Para habilitar UplinkFast (deshabilitado por defecto) se utiliza el siguiente comando:
***spanning-tree uplinkfast***

Sólo utilice UplinkFast en los switches de capa de acceso con enlaces redundantes. Si se activa un switch de tránsito para UplinkFast, se arriesga a una ocurrencia de un bucle en STP. Un switch de tránsito es un switch que conecta tanto el puente raíz y otro interruptor. En la figura, DSW1 es un ejemplo de un interruptor de tránsito si DSW3 es el puente raíz. El único uso aceptable de UplinkFast en el ejemplo está en ASW.

- **BackboneFast**

En el backbone de la red, núcleo o distribución, BackboneFast puede utilizar para agilizar los tiempos de convergencia de nonrapid STP. Cuando se produce un fallo en el enlace indirecto, BackboneFast comprueba si existe un camino alternativo al puente raíz. Un fallo indirecto es cuando un enlace que no está directamente conectado a un switch falla.

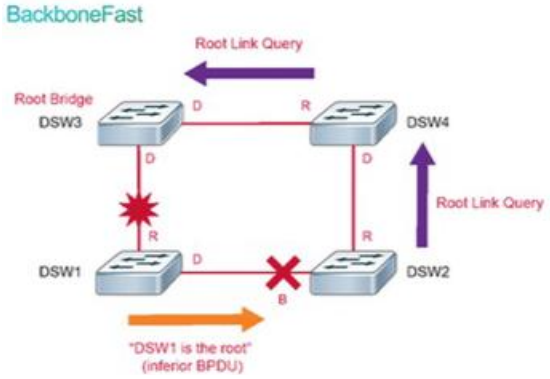



**Figura 15. BackboneFast.**
**Fuente:** CCNP R&S SWITCHING: Implementing IP Switching 300-115 Certification Exam.

DSW3 es el puente raíz y DSW2 es la ruta alternativa bloqueada para DSW3 a DSW1. Cuando el puerto raíz DSW1 falla, DSW1 se declara puente raíz, comienza a enviar BPDU a todos los interruptores a los que está conectado, en este caso, sólo DSW2. Cuando un switch recibe una BPDU inferior en un puerto bloqueado, se ejecuta un procedimiento para validar que todavía tiene una ruta activa para el puente raíz actualmente conocido.

Normalmente, un interruptor debe esperar a que el temporizador “Max Age” expire, antes de responder a las BPDU inferiores. Sin embargo, BackboneFast busca un camino alternativo:

- Si la BPDU inferior llega en un puerto que está bloqueado, el interruptor supone que el puerto raíz y todos los demás puertos bloqueados son un camino alternativo.

- Si la BPDU inferior llega a un puerto que es la raíz, el interruptor supone que todos los puertos bloqueados son un camino alternativo. Si no hay puertos están bloqueados, entonces el interruptor asume que pierde la conectividad con el puente raíz y considera a sí mismo como el puente raíz.

Para habilitar BackboneFast (deshabilitado por defecto) se utiliza el siguiente comando:
***spanning-tree backbonefast***

- **Portfast**

Un PC de usuario final conecta con los switches de capa de acceso. Cuando el PC está encendido, STP tendrá que pasar por todos los estados, blocking, listening, learning, y forwarding. Con los temporizadores STP por defecto, esta transición se llevará a cabo en alrededor de 30 segundos, 15 de la listening a learning, y 15 segundos de learning a forwarding. El PC no será capaz de transmitir o recibir datos antes de que el switch de la transición al puerto de estado de forwarding. ¿Cómo puede afectar a la PC del usuario? El PC puede tener problemas al tratar de adquirir primero las direcciones DHCP, por lo tanto, tendrá que pasar cierto tiempo para que el PC entre en funcionamiento.

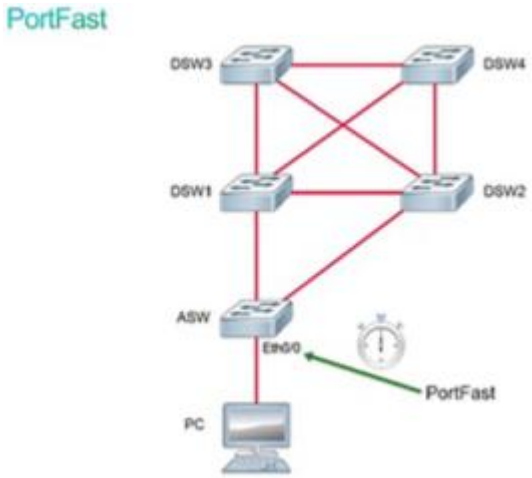



**Figura 16. PortFast.**
**Fuente:** CCNP R&S SWITCHING: Implementing IP Switching 300-115 Certification Exam.

Cuando se habilita PortFast, el puerto pasará inmediatamente de blocking a forwarding. En una gran red, los ordenadores cambian de sitio a menudo, y pueden crear una gran cantidad de TCN (Topology Change Notification) si sus puertos acceso no están configurados con PortFast.

## 2.4. DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP).

DHCP es un protocolo de red que permite a los administradores de red gestionar la asignación y configuración automática de IPs. Sin DHCP, los administradores deben asignar y configurar manualmente las direcciones IP, máscaras de subred, puertas de enlace predeterminadas y así sucesivamente, cosa que puede, en entornos más grandes, convertirse en un problema administrativo excesivo, especialmente si los dispositivos se mueven de un red interna a otra. En un entorno empresarial, un servidor DHCP es normalmente un dispositivo dedicado, mientras que en las implementaciones más pequeñas o alguna sucursal, se puede configurar en un switch o un router.

La configuración de direcciones IPv4 en todos los dispositivos en la red puede ser una tarea onerosa. DHCP reduce en gran medida los gastos generales de administración y ofrece algunas características adicionales, se puede utilizar incluso para asignar una dirección IP específica a un dispositivo, lo cual puede ser útil para los servidores de la red. También hay opciones de DHCP que ofrecen información adicional que puede ser distribuida a los clientes DHCP. Probablemente el ejemplo más común es la opción DHCP 150, el cual se utiliza para asignarle direcciones IP a los teléfonos IP de un servidor TFTP. IPv6 tiene una serie de mecanismos de asignación de direcciones dinámicas, incluyendo configuración automática sin estado, DHCPv6, y DHCPv6 sin estado (también conocido como DHCPv6 Lite).

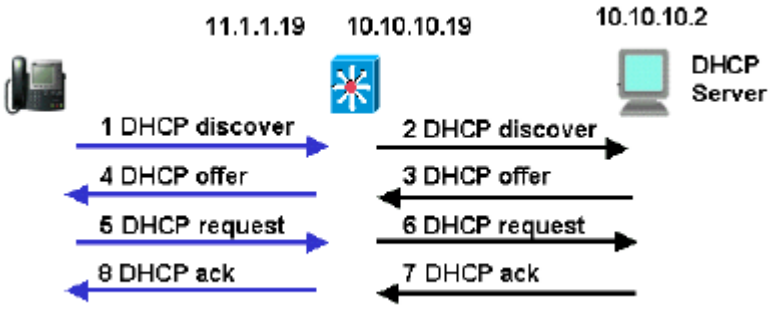



**Figura 17. Dynamic Host Configuration Protocol.**
**Fuente:**http://www.cisco.com/c/dam/en/us/support/docs/ip/dynamic-address-allocation-resolution/19580-dhcp-multintwk-4.gif

DHCP proporciona los parámetros de configuración en los servidores de Internet. Se compone de dos componentes: un protocolo para la entrega del parámetro de configuración específico de host de un servidor DHCP a un host, y el mecanismo de asignación de direcciones de red a hosts. Se basa en el modelo cliente/servidor, donde los servidores DHCP designados asignan las direcciones de red y entregan los parámetros de configuración IP

de forma dinámica. Por defecto, los switches multicapa Cisco que ejecutan el software Cisco incluyen servidor DHCP y el software relay agent.

Los switches de distribución de múltiples capas a menudo actúan como puertas de enlace de capa 3 para clientes que se conectan a las distintas VLAN en los switches de acceso, por lo tanto, el servicio DHCP puede ser proporcionado directamente por el switch de distribución. Por otra parte, los servicios DHCP se pueden concentrar en un servidor DHCP externo dedicado. En ese caso, los switches de distribución deben redirigir las peticiones entrantes del cliente DHCP en el servidor DHCP externo.

### 2.4.1. DHCP relay

El servicio DHCP no tiene que estar configurado directamente en el switch multicapa, muchas redes utilizan un servidor DHCP centralizado. En este caso, el switch multicapa puede redirigir las peticiones DHCP al servidor DHCP corporativo.

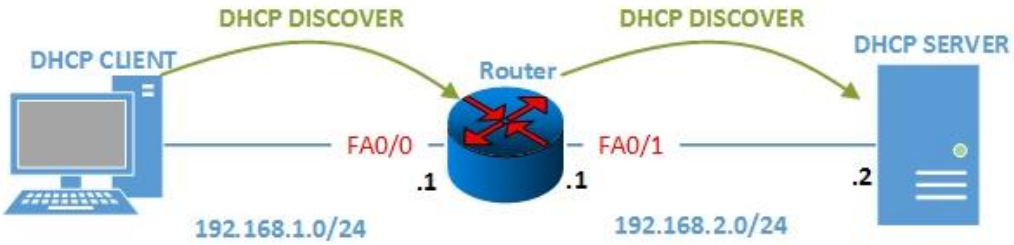



**Figura 18. DHCP Relay.**
**Fuente:** http://configNetworks.com/wp-content/uploads/2014/09/Dessin2DISCOVER.jpg

En esta configuración, se involucran varios elementos:

- El switch multicapa debe tener una dirección IP de capa 3 que recibirá la solicitud DHCP cliente. Esta dirección puede ser un puerto del router o un SVI.
- El comando ***ip helper-address*** debe ser configurador en la interfaz del switch multicapa.

Cuando el switch recibe una solicitud DHCP en la forma de cliente, deja pasar el pedido como un mensaje *unicast* a la dirección IP que se especifica en el comando ***ip helper-address***. Con esta función, el switch transmite el diálogo entre el cliente y el servidor DHCP.

### 2.4.2. Opciones de DHCP

Los parámetros de configuración avanzados y otra información de control son llevados en ítems con etiquetas también llamados “opciones DHCP”. A continuación se muestran algunas opciones DHCP comunes.

- **Opción 43:** Opciones de “*vendor-encapsulation*”, que permiten a los proveedores tener su propia lista de opciones en el servidor. Por ejemplo, se puede utilizar para decirle a una AP ligera en donde está el DLC.

- **Opción 69:** Servidor SMTP.

- **Opción 70:** Servidor POP3.

- **Opción 150:** Servidor TFTP.

## 2.5. FIRST HOP REDUNDANCY PROTOCOL (FHRP).

FHRP es un protocolo de red diseñado para proteger la puerta de enlace predeterminada al permitir que dos o más routers o switches de Capa 3 proporcionen una copia de seguridad para esa dirección. Si falla un dispositivo de primer salto, el enrutador de respaldo se hará cargo de la dirección, por defecto en pocos segundos. FHRP es una categoría de protocolos que incluye HSRP, VRRP y GLBP. Los tres protocolos tienen versiones que admiten la redundancia del primer salto no sólo en entornos IPv4, sino también en entornos IPv6. Sin embargo, no todos los las plataformas y versiones de Cisco IOS admiten todos estos tres protocolos para IPv4 e IPv6.

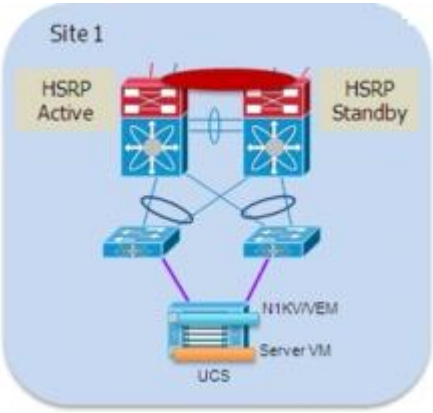



**Figura 19. First Hop Redundancy Protocol.**
**Fuente:** http://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Data_Center/DCI/4-0/EMC/EMC_2.fm/_jcr_content/renditions/EMC_2-07.jpg

Con la redundancia de primer salto, un conjunto de enrutadores y switches de capa 3 trabaja en conjunto para presentar la ilusión de un único enrutador virtual a los hosts de la LAN. Al compartir una dirección IP y una dirección MAC (capa 2), dos o más enrutadores pueden actuar como un solo enrutador "virtual". La dirección IP del enrutador virtual se configura como la puerta de enlace predeterminada para las estaciones de trabajo en una subred específica. Cuando se deben enviar tramas desde la estación de trabajo a la puerta de enlace predeterminada, la estación de trabajo utiliza ARP para resolver la dirección MAC asociada con la dirección IP de la puerta de enlace predeterminada. La resolución ARP devolverá la dirección MAC del enrutador virtual. Las tramas que se envían a la dirección MAC del router virtual pueden ser procesadas físicamente por un enrutador físico activo que forma parte de ese grupo de enrutador virtual.

El protocolo de redundancia proporciona el mecanismo para determinar qué enrutador debe asumir el papel activo en el reenvío de tráfico y determinar

cuándo ese rol debe ser asumido por el router en espera. La trasmisión de un enrutador de reenvío a otro es transparente para los hosts de red.

### 2.5.1. Hot standby router Protocol (HSRP)

Una red de alta disponibilidad ofrece medios alternativos para acceder a todas las rutas de infraestructura y servidores clave en todo momento. HSRP es una de las características que se pueden configurar para proporcionar redundancia de puerta de enlace predeterminada a los hosts de red. La optimización HSRP proporciona una conmutación por error inmediata o específica de enlace, así como un mecanismo de recuperación.

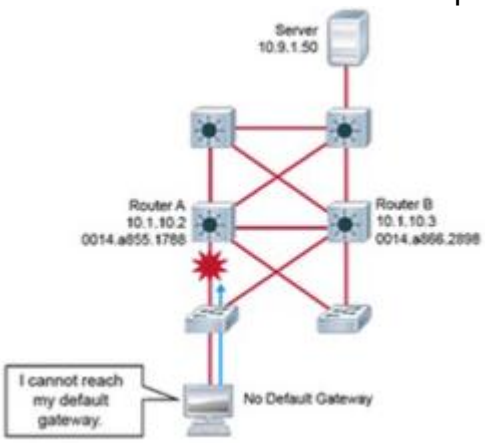



**Figura 20. Hot Standby Router Protocol.**
**Fuente:** CCNP R&S SWITCHING: Implementing IP Switching 300-115 Certification Exam.

En la figura, tanto el enrutador A como el enrutador B están conectados a la red 10.1.10.0/24 y están anunciando con el protocolo de enrutamiento. Todos los paquetes que están destinados a la red 10.1.10.0/24 son enrutados al enrutador A. Si el enrutador A no está disponible, el protocolo de enrutamiento convergerá dinámicamente y los paquetes serán enviados al enrutador B. La redundancia se consigue así con un protocolo de enrutamiento dinámico.

Sin embargo, las estaciones de trabajo de las subredes 10.1.10.0/24, como la mayoría de las estaciones de trabajo, servidores, impresoras y otros hosts de redes, no admiten protocolos de enrutamiento dinámico. Cada vez que un host de red desea comunicarse con un host que se encuentra en una subred distinta, los paquetes deben ser retransmitidos a través de un dispositivo de Capa 3 (un enrutador o un conmutador de Capa 3). Los paquetes que se destinan a otra subred se envían a un dispositivo de Capa 3 mediante un proxy ARP o la configuración de puerta de enlace determinada.

Con la técnica proxy ARP, un dispositivo de Capa 3 ofrece su propia dirección MAC en respuesta a una consulta ARP a una dirección MAC que

existe fuera de la subred de origen, aceptando así todos los paquetes subsiguientes destinados a esa dirección, dirigiéndolos a otra subred. La técnica proxy ARP no tiene mecanismos de repliegue, y la introducción de múltiples routers que utilizan esta técnica en la misma subred provocará problemas como el MAC flapping.

Los hosts de red se configuran con una única dirección IP de puerta de enlace predeterminada. Todos los paquetes que se destinan a otra subred se envían a la dirección IP de puerta de enlace predeterminada, que no cambia cuando se producen cambios de topología de red. Si el enrutador cuya dirección IP actúa como puerta de enlace predeterminada de los hosts de red falla, un host de red no podrá enviar paquetes a otra subred, lo que efectivamente lo desconectará del resto de la red. Incluso si existe un enrutador redundante que podría servir como puerta de enlace predeterminada para esa subred, no existe un método dinámico mediante el cual estos dispositivos pueden determinar la dirección de una nueva puerta de enlace predeterminada.

## 2.6. OPEN SHORTEST PATH FIRST (OSPF).

OSPF es un protocolo de enrutamiento IGP (Interior Gateway Protocol) que utiliza estados de enlace en lugar de vectores de distancia para la selección de ruta. OSPF utiliza un algoritmo de estado de enlace para construir y calcular la ruta más corta a todos los destinos conocidos. Cada router en un área OSPF contiene una base de datos de estado de enlace idéntica, que es una lista de cada una de las interfaces utilizables en los router y vecinos alcanzables. A nivel alto, la operación OSPF consta de tres elementos principales: descubrimiento de vecinos, intercambio de información de estado de enlace y cálculo de la mejor ruta.

Para calcular la mejor ruta OSPF utiliza SPF (Shortest Path First) o el algoritmo de Dijkstra. La información de entrada para el cálculo de SPF es la información del estado de enlace, que se intercambia entre routers a través de diferentes tipos de mensajes OSPF. Estos tipos de mensajes ayudan a mejorar la convergencia y la escalabilidad en los despliegues OSPF multi-areas.

OSPF es uno de los protocolos IGP más comúnmente utilizados en redes IP. OPSFv2 es un una versión de estándar abierto que proporciona enrutamiento para IPv4 y OSPFv3 ofrece algunas mejoras para IPv6. OSPF propaga anuncios de estado de enlace en lugar de actualizaciones de la tabla de enrutamiento, dado que se intercambian LSAs en lugar de todas las tablas de enrutamiento, las redes OSPF convergen de manera oportuna. OSPF también soporta varios tipos de red diferentes, lo que le permite configurar OSPF sobre una variedad de diferentes tecnologías de red subyacentes.

### 2.6.1. Funciones de OPSF

OSPF fue desarrollado por el IETF para superar las limitaciones de los protocolos de vectores de distancia. Una de las principales razones por las que OSPF está ampliamente desplegado en redes empresariales, es el hecho de que es un estándar abierto - OSPF no es propietario.

La versión 1 del protocolo se describe en RFC 1131. La versión actual utilizada para IPv4 versión 2 se especifica en FRC 1247 y 2328. OPSF versión 3, que se utiliza en las redes IPV6, se especifica en RFC 5340.

OSPF ofrece un mayor nivel de escalabilidad y una convergencia rápida. A pesar de que su configuración es relativamente simple en las redes pequeñas y medianas, la implementación OSPF y la solución de problemas en redes a gran escala puede representar un verdadero desafío.

**Las características más importantes del protocolo OSPF son:**

- ***Transporte independiente:*** OSPF funciona en la parte superior de IP y utiliza el número de protocolo 89. No depende de las funciones de TCP o UDP.

- ***Uso eficiente de las actualizaciones:*** Cuando un enrutador OSPF descubre por primera vez un nuevo vecino, enviará una actualización completa con toda la información de estado del enlace conocida. Todos los routers dentro de un área OSPF deben tener información de estado de enlace sincronizada e idéntica en sus bases de datos OSPF. Cuando una red OSPF está en un estado convergente y aparece un nuevo enlace o un enlace no está disponible, un enrutador OSPF enviará sólo una actualización parcial a todos sus vecinos. Esta actualización se inundará a todos los enrutadores OSPF dentro de un área.

- ***Métrica:*** OSPF utiliza una métrica que se basa en el coste acumulativo de todas las interfaces de salida de origen a destino. El costo de la interfaz es inversamente proporcional al ancho de banda de la interfaz y se puede configurar explícitamente.

- ***Actualización de dirección de destino:*** OSPF utiliza multidifusión y unidifusión, en lugar de difusión. Las direcciones de multidifusión utilizadas para OSPF son 224.0.0.5 para enviar información a todos los routers OSPF y 224.0.0.6 para enviar información a routers DR o BDR. Si la red subyacente no tiene capacidades de difusión, debe establecer relaciones de vecino OSPF utilizando *unicast*.

- ***Compatibilidad con VLSM:*** OSPF es un protocolo de enrutamiento sin clases y soporta VSLM (máscara de subred de tamaño variable). Transporta la información de las máscaras de subred en las actualizaciones de enrutamiento.

- ***Autenticación:*** OSPF es compatible con autenticación cleartext, MD5 y SHA.

### 2.6.2. Descripción general de la operación de OSPF

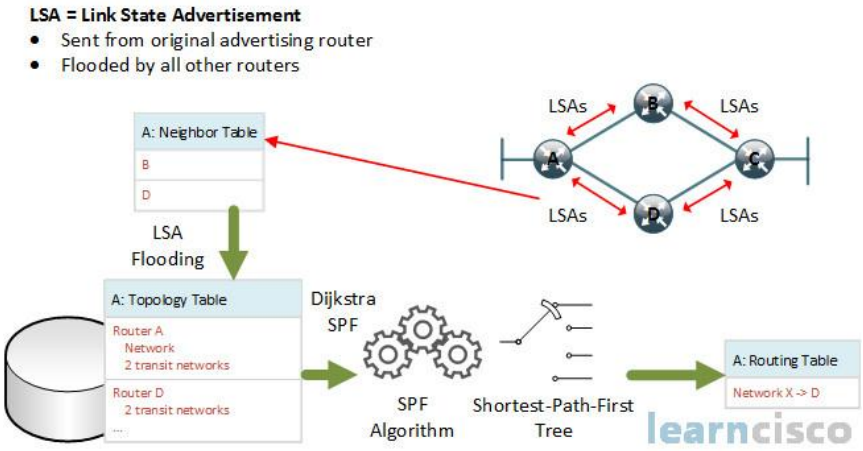



**Figura 21. Descripción de OSPF**
**Fuente:** http://www.learncisco.net/courses/icnd-2/an-overview-of-ospf/ospf-data-overview.html

A un alto nivel, la operación OSPF se puede dividir en tres pasos distintos. En el primer paso, el enrutador OSPF debe descubrir todos los enrutadores vecinos que hablan OSPF en las interfaces directamente conectadas. Para establecer relaciones de vecinos, OSPF utiliza pequeños paquetes de “hello”, similares a EIGRP. Antes de que dos enrutadores directamente conectados se conviertan en vecinos OSPF, deben estar de acuerdo en determinados parámetros especificados en el paquete “hello”. Una vez que dos enrutadores OSPF establecen vecindad, el segundo paso puede comenzar.

En el segundo paso de la operación OSPF, el enrutador intercambia información de estado de enlace que describe la topología de la red dentro de un área OSPF. La información de estado de enlace, transmitida en forma de LSA, se inunda a través de un área OSPF hasta que todos los routers tienen entradas idénticas almacenadas en sus LSDB. Las LSAs recibidos de los vecinos se utilizan en el enrutador local para construir la imagen de la topología de la red de la perspectiva del enrutador local. La información contenida en LSA incluye el identificador de cada enrutador (router ID), la interfaz, la dirección IP, la máscara, la subred y una lista de todos los routers accesibles en cada interfaz.

Una vez que los LSDBs en todos los routers dentro de un área están sincronizados y tienen entradas de base de datos idénticas, el último paso puede comenzar, el mejor cálculo de ruta. Para calcular la mejor trayectoria a la destinación dada, OSPF utiliza SPF o el algoritmo de Dijkstra. El algoritmo SPF analiza y compara todos los posibles caminos hacia el destino desde la perspectiva del router local y selecciona el que tiene la menor métrica

(coste). Esta ruta, junto con el salto siguiente y la interfaz saliente al destino, es un candidato para ser colocada en la tabla de enrutamiento.

### 2.6.3. Estructura jerárquica de OPSF.

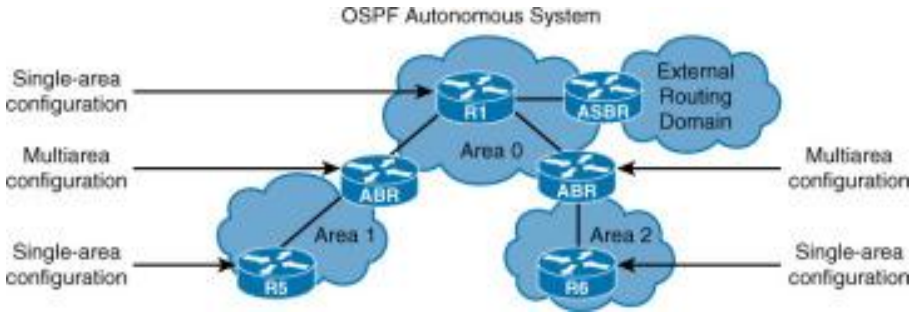



**Figura 22. Estructura jerárquica de OSPF**
**Fuente:** http://www.ciscopress.com/articles/article.asp?p=2294214

Si se ejecuta OSPF en una red simple, el número de routers y enlaces es pequeño y las mejores rutas a todos los destinos se determinan fácilmente. Sin embargo, la información necesaria para describir redes más grandes con varios enrutadores y enlaces puede llegar a ser compleja. Los cálculos de SPF que comparan todas las rutas posibles para routers pueden convertirse fácilmente en un cálculo complejo y lento.

Uno de los principales métodos para reducir la complejidad y tamaño de la base de datos de información de estado de enlace es dividir la red OSPF en unidades más pequeñas denominadas áreas. Esto también reduce el tiempo que tarda el algoritmo SPF en ejecutarse. Todos los routers OSPF dentro de un área deben tener entradas idénticas dentro de sus respectivos LSDB. Dentro de un área, los enrutadores intercambian información de estado-enlace. Sin embargo, la información transmitida de un área a otra contiene sólo detalles de resumen de las entradas de base de datos de estado de enlace y no contiene detalles de topología sobre el área de origen.

*OSPF utiliza una jerarquía de área de dos capas:*

*Área de "backbone", área del tránsito, o área 0*: Los requisitos principales para el área de *backbone* son que debe conectar con todas las áreas que no hacen parte del *backbone*, y debe ser siempre contiguo, es decir, no pueden estar separadas. Generalmente, los usuarios finales no se encuentran en un área del *backbone*.

*Áreas non-backbone:* La función principal de estas áreas es conectar usuarios finales y recursos. Estas áreas se establecen generalmente de

acuerdo con agrupaciones funcionales o geográficas. El tráfico entre las diferentes áreas debe pasar por el área de *backbone*.

En la topología multiarea, hay algunos términos OSPF comúnmente usados:

- ***ABR:*** Un enrutador que tiene interfaces conectadas a al menos dos áreas OSPF diferentes, incluyendo el área de *backbone*. Los ABRs contienen información LSDB para cada área, hacen cálculos de ruta para cada área y anuncian información de enrutamiento entre área.

- ***ASBR:*** Un ASBR es un enrutador que tiene al menos una de sus interfaces conectada a un área OSPF y al menos una de sus interfaces conectada a un dominio externo que no es OSPF.

- ***Enrutador interno:*** Un enrutador que tiene todas sus interfaces conectadas a un solo área OSPF. Este enrutador es completamente interno al área.

- ***Enrutador de backbone:*** Un enrutador que tiene al menos una interfaz conectada al área de *backbone* o área 0.

**El número óptimo de routers por área varía en función de factores tales como la estabilidad de la red, pero la recomendación general es no tener más de 50 routers.*

### 2.6.4. Limitaciones de diseño de OSPF

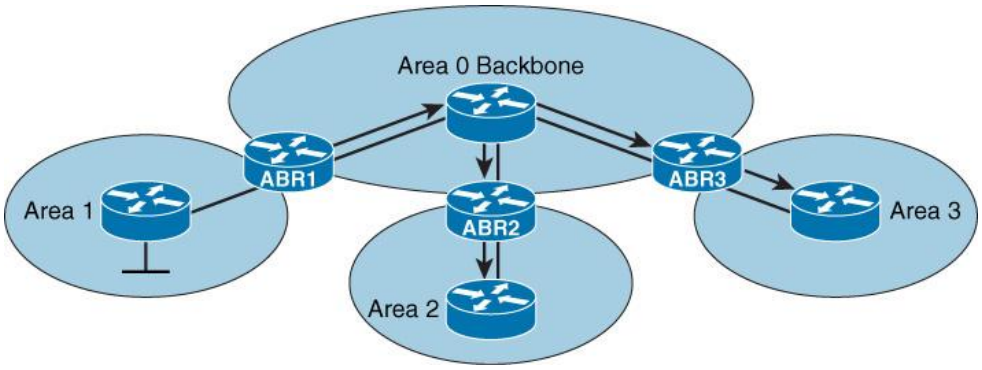



**Figura 23. Limitaciones de OSPF**
**Fuente:** http://www.ciscopress.com/articles/article.asp?p=2294214

OSPF tiene restricciones especiales cuando se configuran varias áreas en un OSPF AS (Sistema Autónomo). Si más de un área está configurada, una de estas áreas tiene que ser el área 0. Se llama el área de "*backbone*".

Al diseñar redes, es una buena práctica empezar con la capa central, que se convierte en área 0, y expandir a otras áreas más tarde.

El área de *backbone* tiene que estar en el centro de todas las demás áreas y las otras áreas tienen que estar conectadas al *backbone*. La razón principal es que OSPF espera que todas las áreas inyecten información de enrutamiento en el área de *backbone*, la cual se encarga de distribuir esa información a otras áreas.

Otro requisito importante para el área de *backbone* es que debe ser contiguo. En otras palabras, no se permite dividir el área 0.

### 2.6.5. Tipos de mensajes de OSPF

OSPF utiliza cinco tipos de paquetes de protocolo de enrutamiento que comparten una cabecera de protocolo común. Cada paquete OSPF se encapsula directamente en la cabecera IP. El número de protocolo IP para OSPF es 89.

- ***Hello Packet:*** se usa para descubrir, construir y mantener las adyacencias vecinas OSPF. Para establecer la adyacencia, los pares de OSPF en ambos lados del enlace deben estar de acuerdo en algunos parámetros contenidos en el paquete “hello”.

- ***Paquete DBD:*** Cuando la vecindad OSPF ya está establecida, un paquete DBD se utiliza para describir el LSDB para que los routers puedan comparar si las bases de datos están sincronizados.

- ***Paquete de LSR:*** Cuando el proceso de sincronización de la base de datos ha finalizado, es posible que el enrutador siga teniendo una lista de LSA que faltan en su base de datos. El enrutador enviará un paquete LSR para informar a los vecinos de OSPF que devolverán la versión más reciente de los LSA perdidos.

- ***Paquete LSU:*** Se utiliza cuando se inundan LSAs y se envían respuestas LSA a paquetes LSR. Se envía sólo a los vecinos directamente conectados que han solicitado anteriormente LSAs en forma de paquetes LSR. En caso de inundación, los routers vecinos son responsables de volver a encapsular la información LSA recibida en nuevos paquetes LSU.

    - ***Paquete LSAck:*** Se utiliza para hacer la inundación de LSAs confiable. Cada LSA recibido debe ser explícitamente reconocido. Se pueden reconocer varios LSA en un solo paquete LSAck.

# PARTE III

Desarrollo de la Propuesta

# **CAPÍTULO 3**
# DESARROLLO DE LA PROPUESTA DE MEJORAMIENTO

*En el siguiente capítulo se desarrolla la propuesta de mejoramiento de la red del cliente de telecomunicaciones. Se muestra la topología actual y señalan sus falencias para luego realizar los diferentes planteamientos para el mejoramiento de la misma.*

## 3.1. TOPOLOGÍA DE RED DEL CLIENTE DE TELECOMUNICACIONES

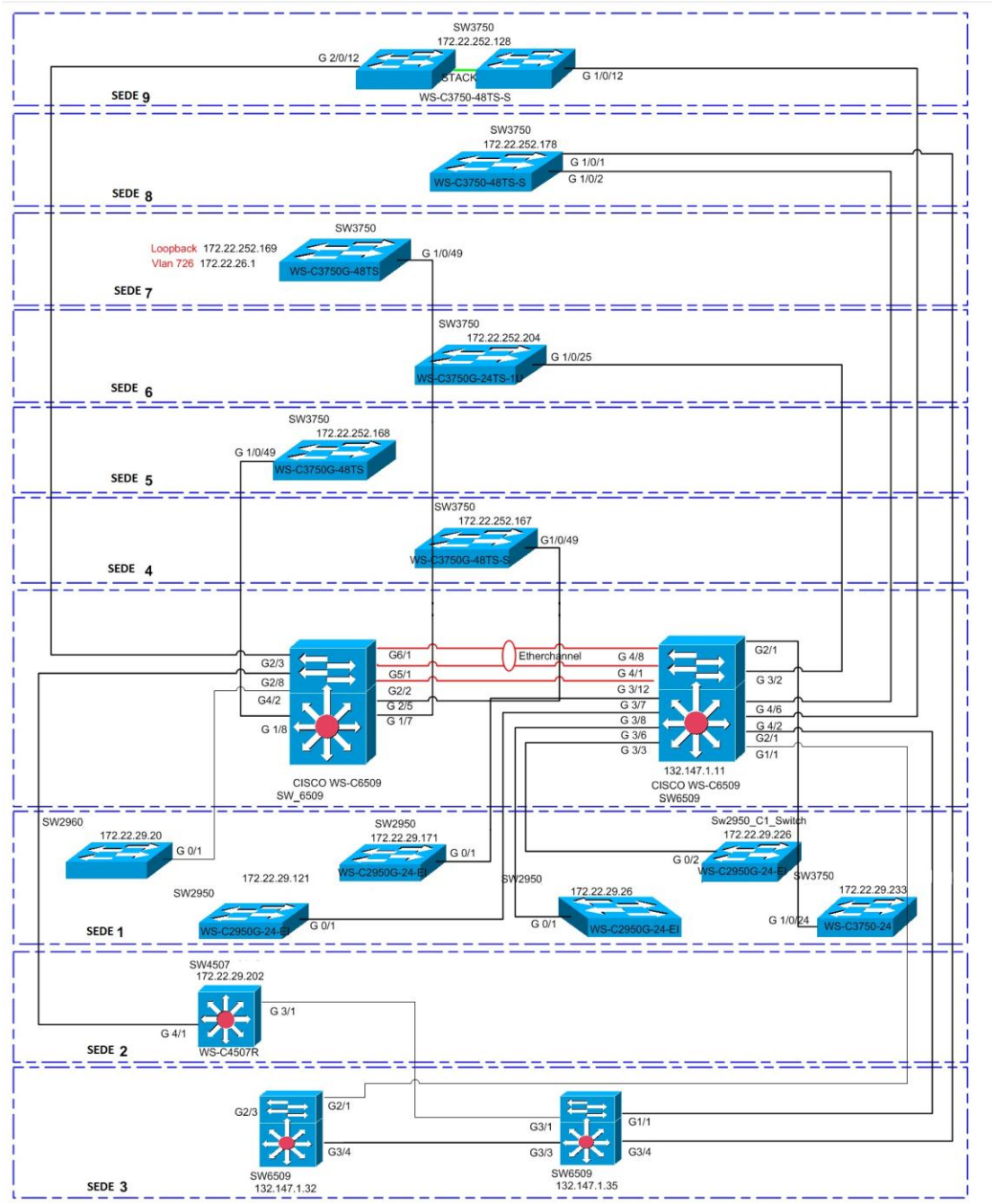



**Figura 24. Topología del Cliente de Telecomunicaciones**
**Fuente:** Diagrama de topología de red elaborado en Microsoft Visio Professional.

La red del cliente cuenta con 9 sedes y 1 Datacenter, el cual se encuentra ubicado geográficamente en el mismo edifico de la sede 1.

El Datacenter está compuesto por 2 Switches multicapa Cisco WS-6509 que a su vez actúan como componentes de Core, los cuales se encuentran conectados mediante enlaces redundantes a los switches de distribución que están compuestos por modelos SW 6509, 3750, 2950, 2960 y 4507.

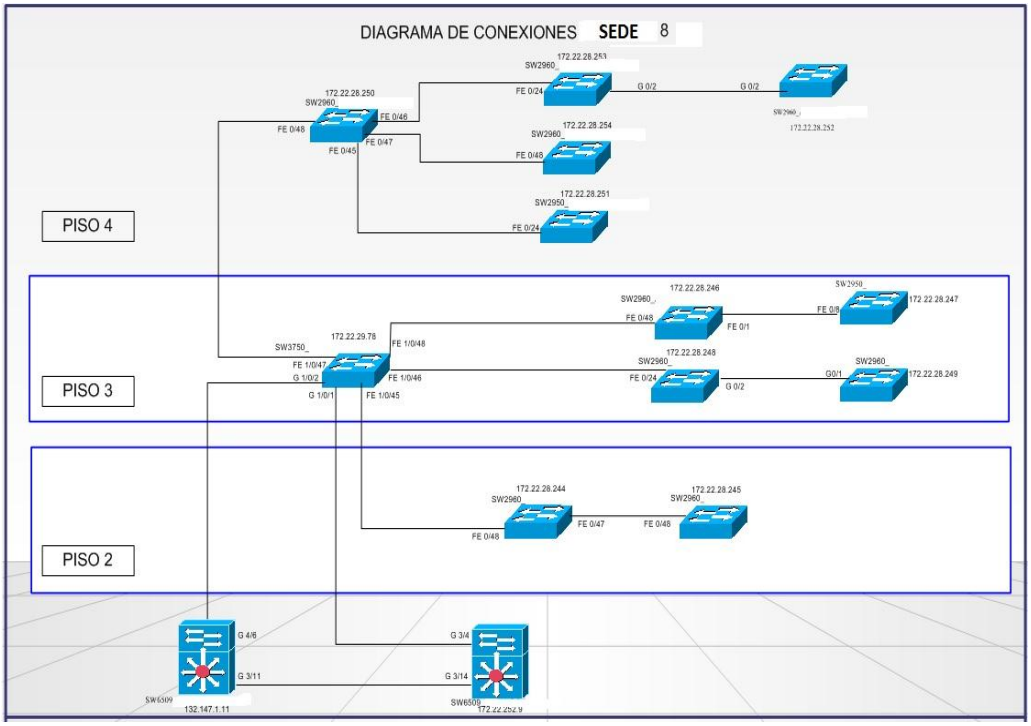



**Figura 25. Topología de una de las sedes del cliente**
**Fuente:** Diagrama de topología de red elaborado en Microsoft Visio Professional.

Este es el ejemplo de la topología de una de las sedes del cliente. Existen 2 componentes de Core conectados un switch de distribución. Los componentes de acceso son switches SW 2960 de capa 2 (11 en total para esta sede) con un total de 48 puertos Ethernet 10/100/1000 Mbps cada uno, lo que se traduce a la interconexión de hasta 528 usuarios o equipos terminales en esta sede.

### 3.1.1. Descripción de los elementos de red de Core y Distribución

| Descripción | Cantidad |
|---|---|
| SW 3750 | 8 |
| SW 6509 | 4 |
| SW 2950 | 4 |
| SW 2960 | 1 |
| SW 4507 | 1 |

## 3.2 ANÁLISIS DE LA ESTUCTURA DE RED

Es muy común ver en el campus empresarial, topologías de red como la que presenta el cliente de telecomunicaciones que se muestra a continuación.

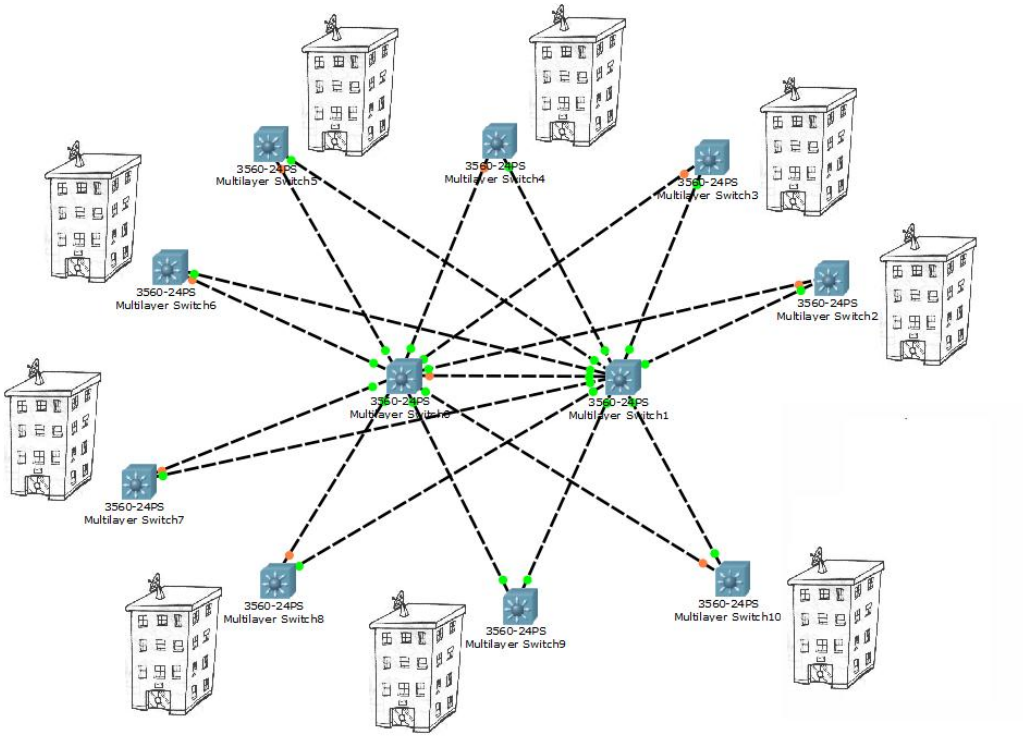



**Figura 26. Estructura de la red del cliente**
**Fuente:** Estructura de la red de core y distribución elaborado en Cisco Packet Tracer.

Para poder estudiar mejor el funcionamiento de la red, se hizo un esquema básico con el programa de simulación de redes Cisco Packet Tracer. Se tiene dos equipos multicapa Cisco WS-C6509 de alta capacidad para recibir todo el tráfico entre las sedes del cliente y 9 switches de capa 2 para conmutar el tráfico en cada una de las sedes.

### 3.2.1. Descripción de la red del cliente

- El tráfico de datos en toda la red se hace a nivel de capa 2. Se tiene una arquitectura como la siguiente.

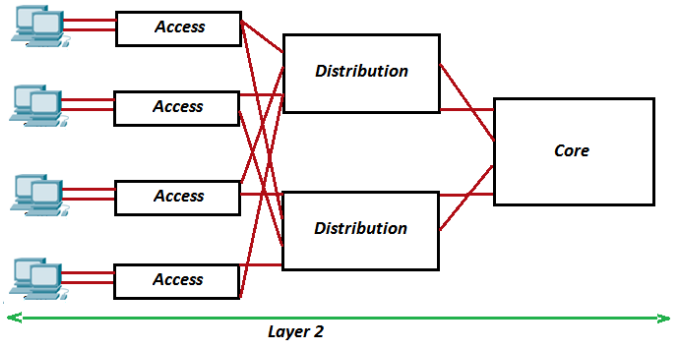



**Figura 27. Modelo de configuración del cliente.**
**Fuente:** Elaboración propia.

- Utiliza una implementación de VLANs de extremo a extremo.

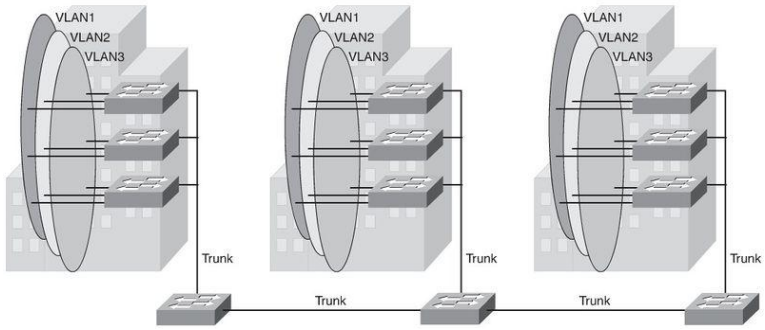



**Figura 28. Implementación de VLANs dentro del cliente.**
**Fuente:** http://ciscodocuments.blogspot.com.co/2011/05/chapter-02-implementing-VLANs-in-campus.html

En cada sede se encuentran conectados servidores a los switches de distribución con información del cliente y resolución de direcciones DHCP.

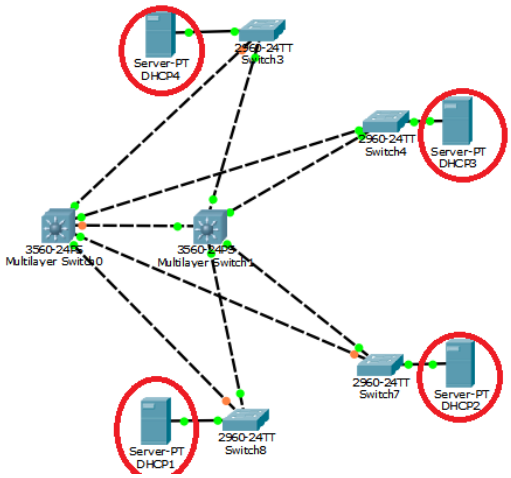



**Figura 29.Ubicación de servidores dentro de la red de cliente**
**Fuente:** Elaboración propia.

- El enrutamiento InterVLAN es llevado a cabo por los equipo de core, siendo estos las puerta de enlace predeterminada para salir a segmentos de red diferentes. Uno de los dos equipos de core se encarga de ser el Gateway predeterminado para algunas sede y el otro equipo para demás.

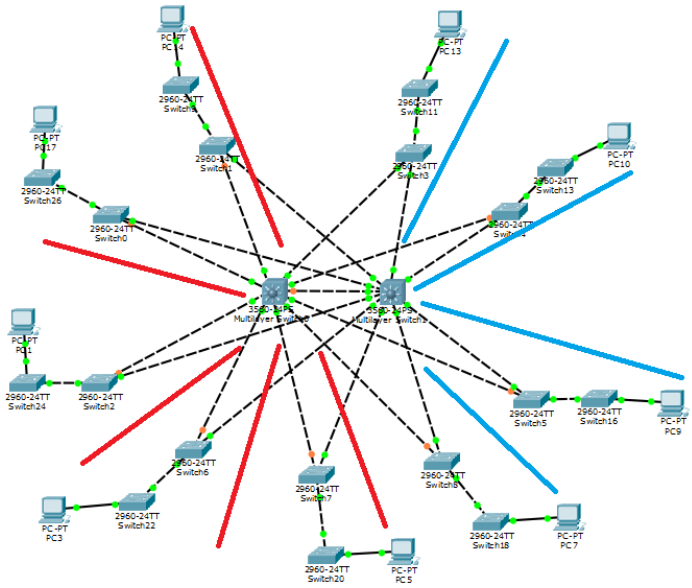


**Figura 30. Configuración de los Gateways.**
**Fuente:** Elaboración propia.

Se muestra a continuación la configuración de los switches de distribución y se muestra #show running-config del mismo con parámetros de configuración presentes.

**Por temas de confidencialidad se censuran algunas líneas "xxxx".*

```
aaa session-id common
clock timezone COL -5
switch 1 provision xxxx// Switches en el stack
switch 2 provision xxxx
system mtu routing 1500//Unidad maxima de transferencia en bytes
vtp domain xxxx// Dominio de Vtp
vtp mode client//Modo de Vtp cliente
ip subnet-zero
ip routing//habilitado el enrutamiento, para este caso interVLAN
no ip domain-lookup
!
!
!
no file verify auto
!
spanning-tree mode rapid-pvst//Modo por defecto de STP
spanning-tree extend system-id
!
VLAN internal allocation policy ascending
!
VLAN 726//Ejemplo de la configuración de una de las VLAN presentes
 name Red_LAN_usuarios_xxxx
!
!
interface Loopback0//Interfaz de red virtual loopback
 ip address 17x.xx.xxx.xx 255.255.255.255
!
interface GigabitEthernet1/0/1
 switchport access VLAN 726//VLAN 726 configurada en modo trunk
 switchport mode access
 !
interface GigabitEthernet1/0/43
 switchport access VLAN 726
 switchport mode access
!
interface GigabitEthernet1/0/44
 description Conexion Trunk hacia SW2960_xxxx Fa 0/48
 switchport trunk encapsulation dot1q//Protocolo IEE 802.1Q-Trunking
 switchport trunk allowed VLAN 726
 switchport mode trunk
 shutdown
!
interface GigabitEthernet1/0/45
```

```
 description Conexion Trunk hacia SW2960_xxxx Fa 0/48
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 726
 switchport mode trunk
!interface VLAN1
 no ip address
 shutdown
!
interface VLAN726
 description VLAN para el edificio xxxx 7
 ip address 172.22.26.1 255.255.255.0
 ip helper-address 172.22.83.72
 ip helper-address 172.22.103.201
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
!
router ospf 1
 log-adjacency-changes
```

Este tipo de práctica es aceptable para redes en las cuales no se tienen muchos equipos debido al poco procesamiento requiere el tráfico de capa 2 en los equipos de red, pero para redes tan robustas como la que se presenta no es conveniente ya que se tienen hasta 528 usuarios terminales en cada sede lo que sumaría un aproximado total de 4752 usuarios terminales. Si bien se sabe que una de las principales características de los switches es dividir una LAN en múltiples dominios de colisión es imposible filtrar el tráfico de difusión, *broadcast*, *multicast* y tramas cuyo destino aún no se encuentro incluido en las tablas de direccionamiento, sumado a esto, se tienen enlaces redundantes entre los switches de cada sede y los equipos de core, lo que genera un alto procesamiento en los equipos de red si todos los equipos terminales se encuentran activos y no se cuenta con la configuración adecuada de tecnologías como STP.

### 3.2.2. Problemas detectados en la red

- **Tormentas de *Broadcast*:** Cada switch en una red redundante envía tramas de difusión sin fin, estos envían tramas de *broadcast* a todos los puertos excepto en el cual la trama fue recibida, formando un bucle en todas las direcciones.

- **Transmisión de Múltiples Tramas:** Múltiples copias de la misma trama de *unicast* pueden ser entregados a una red de destino, lo cual puede causar problemas con el protocolo de recepción. muchos protocolos esperan recibir una sola copia de cada transmisión por lo que múltiples copias de la misma trama puede producir errores irrecuperables.

- **Inestabilidad de la base de datos MAC:** Este problema se produce cuando muchas copias de la misma trama están siendo recibidas por diferentes puertos en el switch. La tabla de direcciones MAC asigna la dirección MAC de origen en un paquete de recibido en la interfaz que se recibió. Si se produce un bucle, la misma dirección MAC de origen podría ser vista en múltiples interfaces, causando inestabilidad. el reenvío de datos puede verse afectado porque el switch consume muchos de sus recursos intentando resolver a la inestabilidad en la tabla de direcciones MAC.

Para ver los efectos del tráfico de *broadcast* en una red, se muestra una simulación utilizando el programa “Mausezahn” el cual es un programa de simulación de redes y contiene un generador de paquetes.

Para la práctica se utilizó u switch cisco WS-C2960-24TC-L y se generó un conjunto de paquetes para evidenciar la carga que sufre la CPU del equipo. La topología utilizada es la siguiente. [4]

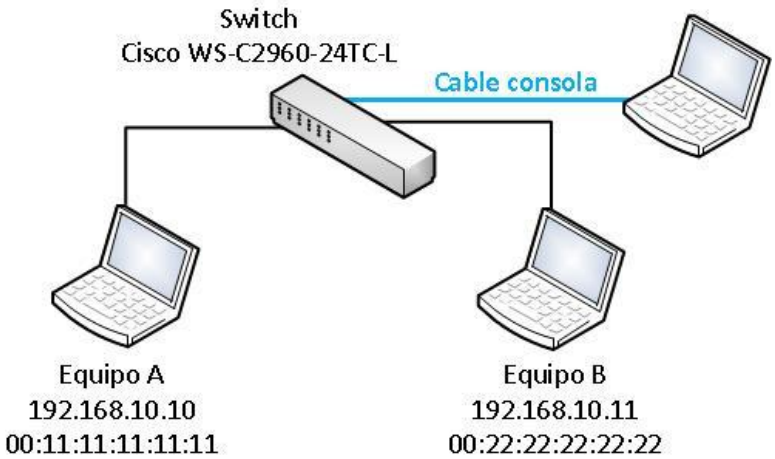



**Figura 31. Topología en Mausezhan.**
**Fuente:** https://enredandoconredes.com/2012/06/20/trafico-broadcast/>

Se generaron paquetes de “ARP replies” del equipo A al equipo B.

| | | | | | | |
|---|---|---|---|---|---|---|
| 63873 | 0.999550 | Schaffne_22:22:22 | Intel_11:11:11 | ARP | 42 | 192.168.10.11 is at 00:22:22:22:22:22 |
| 63874 | 0.999554 | Schaffne_22:22:22 | Intel_11:11:11 | ARP | 42 | 192.168.10.11 is at 00:22:22:22:22:22 |
| 63875 | 0.999557 | Schaffne_22:22:22 | Intel_11:11:11 | ARP | 42 | 192.168.10.11 is at 00:22:22:22:22:22 |
| 63876 | 1.000385 | Schaffne_22:22:22 | Intel_11:11:11 | ARP | 42 | 192.168.10.11 is at 00:22:22:22:22:22 |
| 63877 | 1.000388 | Schaffne_22:22:22 | Intel_11:11:11 | ARP | 42 | 192.168.10.11 is at 00:22:22:22:22:22 |
| 63878 | 1.000394 | Schaffne_22:22:22 | Intel_11:11:11 | ARP | 42 | 192.168.10.11 is at 00:22:22:22:22:22 |
| 63879 | 1.000397 | Schaffne_22:22:22 | Intel_11:11:11 | ARP | 42 | 192.168.10.11 is at 00:22:22:22:22:22 |

**Figura 32. Paquetes ARP replies generados en el simulador.**
**Fuente:** https://enredandoconredes.com/2012/06/20/trafico-broadcast/>

Se puede observar que se produjeron un total de 63876 tramas y se monitorea el consumo de CPU en el Switch.

```
PRUEBAS01#show processes cpu history

                                                                    11111
    5544444444445555544444444444444444444444444444444411111444445
100
 90
 80
 70
 60
 50
 40
 30
 20
 10 **           *****                                      *****      *
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per second (last 60 seconds)
```

**Figura 33. Uso de CPU del switch.**
**Fuente:** https://enredandoconredes.com/2012/06/20/trafico-broadcast/>

Se puede observar el consumo de CPU tuvo un máximo de 11%. Pero si se realiza un “ARP request” para hallar la dirección MAC del equipo A.

| | | | | | | |
|---|---|---|---|---|---|---|
| 15061 | 0.999379 | Intel_11:11:11 | Schaffne_22:22:22 | ARP | 60 | 192.168.10.10 is at 00:11:11:11:11:11 |
| 15062 | 0.999445 | Intel_11:11:11 | Schaffne_22:22:22 | ARP | 60 | 192.168.10.10 is at 00:11:11:11:11:11 |
| 15063 | 1.003636 | Intel_11:11:11 | Schaffne_22:22:22 | ARP | 60 | 192.168.10.10 is at 00:11:11:11:11:11 |
| 15064 | 1.003821 | Schaffne_22:22:22 | Broadcast | ARP | 42 | Who has 192.168.10.10?  Tell 192.168.10.11 |
| 15065 | 1.003848 | Intel_11:11:11 | Schaffne_22:22:22 | ARP | 60 | 192.168.10.10 is at 00:11:11:11:11:11 |

**Figura 34. Paquetes ARP request generados en el simulador.**
**Fuente:** https://enredandoconredes.com/2012/06/20/trafico-broadcast/>

Se envían 15603 tramas en un segundo, es decir, 48,273 menos que con un “ARP replies”, sin embargo el consumo de CPU aumenta a un 80%.

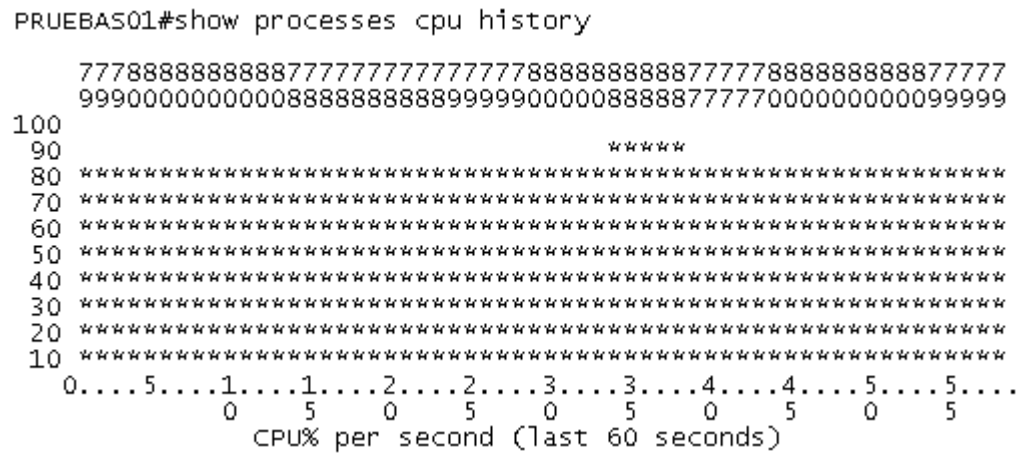



**Figura 35. Uso de CPU en el switch.**

**Fuente:** https://enredandoconredes.com/2012/06/20/trafico-broadcast/>

Si se tiene en cuenta el escenario real de la red del cliente, el tráfico se propaga a todos los switches, por lo que el procesamiento de todos los equipos se verá afectado.

Por esta razón es necesario utilizar las diferentes tecnologías que ofrece Cisco System para evitar casos como estos y seguir las recomendaciones sobre el diseño de redes.

## 3.3. PROPUESTA DE MEJORAMIENTO.

I. **Uno de los principales problemas detectados en la red es la implementación de las VLAN.**

Se tiene una implementación de VLAN extremo a extremo, esto quiere decir que todos los equipos de la red conocen todas las VLAN de toda la red, si bien se manejan 4 tipos de VLAN (Datos, Voz, Servidores y Gestión), cada una se divide en diferentes números de VLAN para las comunicaciones de los diferentes servicios, es decir, existen varias VLAN para Datos, Voz, y los diferentes servidores que alojan información administrativa del cliente, y una única VLAN para la gestión remota de los equipos.

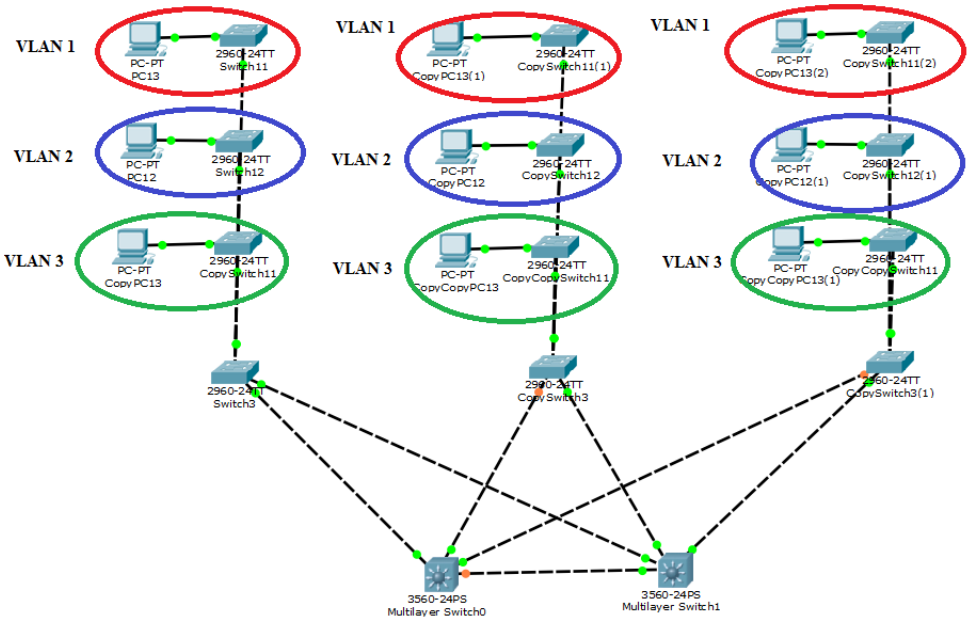



**Figura 36. End-to-end VLAN.**
**Fuente:** Elaboración propia.

Siendo esta la implementación dada, hay que aclarar que para que exista comunicación entre una misma VLAN que existe en una o varias sedes, todo el tráfico pasar por todos los equipos de la red cuando intenta encontrar su destino si aún no está incluido en su tabla ARP, esto incluye una sobrecarga en los equipos de core de la red que son los encargados de intercomunicar las diferentes sedes.

La solución propuesta para evitar esta sobrecarga, es implementar VLANs locales como se muestra en la figura 37.

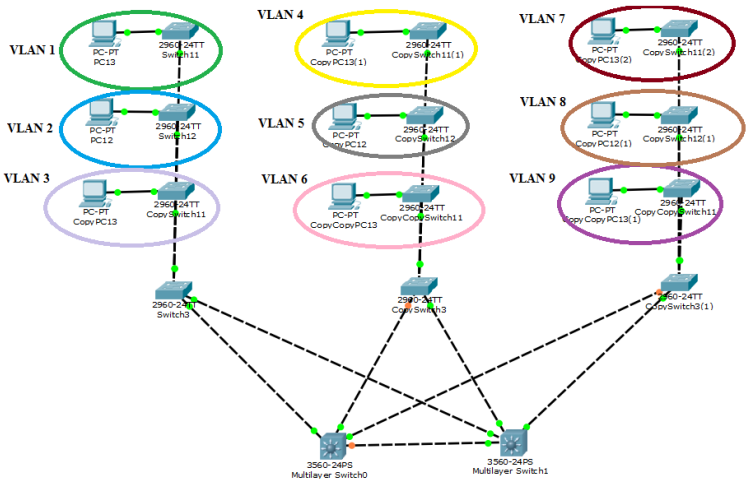



**Figura 37. Local VLAN.**
**Fuente:** http://ciscodocuments.blogspot.com.co/2011/05/chapter-02-implementing-VLANs-in-campus.html

Si bien, debe existir un mecanismo para poder intercomunicar las diferentes VLANs en diferentes segmentos de red, el cual hace parte de otra de las soluciones propuestas para el mejoramiento de la red, se evita que el tráfico se propague a equipos que no necesitan intervenir en el proceso, y en caso de que se quiera comunicar con una VLAN que se encuentra en otra sede, se hace a través de un protocolo IGP, como se propone en la siguiente solución.

II. **El diseño de una red capa 2 presenta diversas desventajas para este caso.**

Si bien, es una práctica común para redes pequeñas que requieren un procesamiento muy bajo en los equipos de red, es común ver subidas de procesamiento en todos los equipos puesto que cualquier trafico debe llegar a todos los equipos para luego encontrar su destino, creándose así una tormenta de *broadcast* debido a que los equipos de *core* deben encontrar su destino mientras los incluye en la tabla ARP.

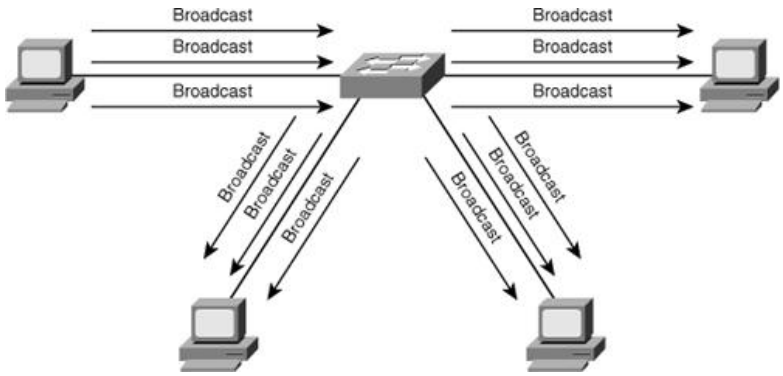



**Figura 38. Trafico de *Broadcast* en una red.**
**Fuente:** http://ciscodocuments.blogspot.com.co/2011/05/chapter-07-lan-san-voice-and-endpoint_9611.html

No se puede cometer este tipo de errores de configuración y diseño si se desea implementar una red más robusta para intercomunicar diferentes sedes en el cliente de telecomunicaciones.

Para estos casos Cisco System propone las siguientes alternativas.

Cuando se diseña la capa de acceso, se pude tener solo enlaces capa 2 o se puede configurar algún tipo de enrutamiento. Cualquiera de los dos diseños tiene sus ventajas y desventajas.

La primera opción es tener conmutación de capa 2 (también conocido como bridging). Las VLAN se terminan en la capa de distribución y la mitad de los enlaces ascendentes se bloquean debido a la operación de spanning-tree.

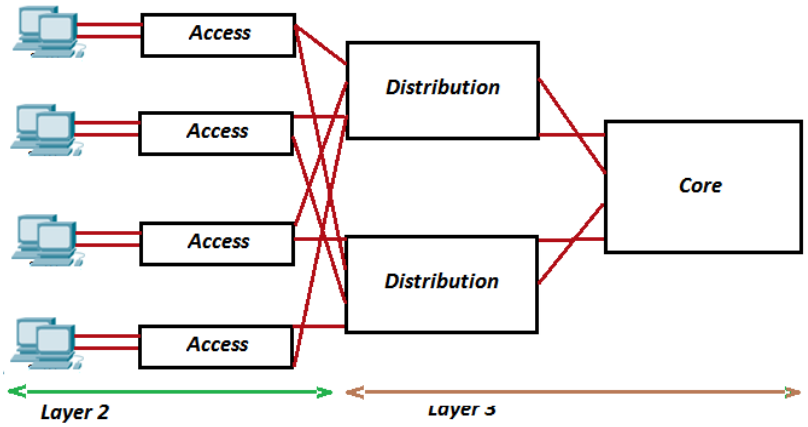



**Figura 39. Modelo de configuración *bridging*.**
**Fuente:** Elaboración propia.

La segunda opción es tener conmutación de Capa 3 (también conocido como *routing*). Las VLAN se terminan en los dispositivos de la capa de acceso. Los enlaces entre los switches de distribución y la capa de acceso son enlaces enrutados y todos los dispositivos de acceso y distribución participarían en el enrutamiento.

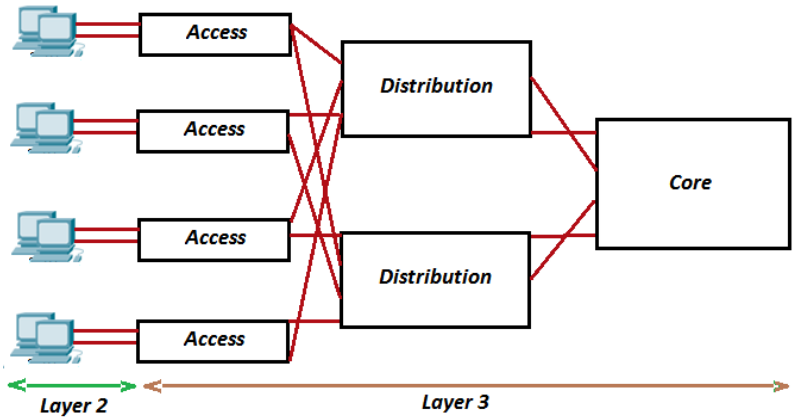



**Figura 40. Modelo de configuración *routing*.**
**Fuente:** Elaboración propia.

El diseño de acceso de capa 2 es una solución tradicional, puesto que es mucho más económico. Sin embargo STP mientras intenta deshacerse de los bucles, bloquea la mitad de los enlaces ascendentes. Un diseño de capa 3 presenta cómo se debería separar el tráfico, por ejemplo, el tráfico de invitados debe permanecer separado de tráfico interno lo cual requiere una planificación cuidadosa. Una VLAN en un dispositivo de acceso de capa 3 no puede propagarse en otro switch de acceso en una parte diferente de su red, cada VLAN es local. Con un diseño de capa 2, puede tener la misma VLAN en varios switches de capa de acceso; sin embargo, no se recomienda la práctica.

La propuesta número 2, es la más conveniente para este caso.

Habilitando un protocolo de enrutamiento IGP como OSPF, entre los enlaces que van entre acceso-distribución-core, ayudan a separar los dominios de *broadcast* y se restringe la comunicación de las VLAN que se encuentran en una misma sede para que el tránsito de *broadcast* y difusión se maneje de manera interna entre los equipos finales y los switches de Acceso y en caso de que se requiera comunicar con un segmento de red o una VLAN que se encuentre en otra sede se haga a través de enrutamiento.

Ventajas que ofrece OSPF para la red del cliente.

- Rápida propagación de los cambios dentro de la red.
- Gracias a que el core de la red se encuentra centralizado contrasta el diseño jerárquico de OSPF en el cual el área 0 se puede configurar en los enlaces entre el core y la distribución.
- Utiliza un algoritmo de estado de enlace lo que facilita la escogencia de la mejor ruta para llegar a su destino.

- Admite máscaras de subred de longitud variable para facilitar la segmentación de la red y de las VLAN del cliente.
- Solo activa actualizaciones en la tabla de enrutamiento sobre los enlaces que han cambiado y no sobre toda la tabla de enrutamiento, lo que permite una mejor escalabilidad de la red.
- Es un estándar abierto que puede ser configurado en equipos de diferentes fabricantes en casa de que se requieran cambios en un futuro,
- No inunda la red en caso de que no existan cambios, los paquetes de "Hello" son los únicos enviados en intervalos de tiempos regulares para comprobar el estado de los enlaces.

III. **Los equipos servidores se encuentran propagados en las diferentes sedes y los clientes de resolución de direcciones DHCP se encuentran configurados en los equipos de distribución.**

La VLAN de servidores junto con todas las VLANs de la red, se encuentran propagadas en toda la red, por lo que se puede tener acceso y configuración a todas ellas desde cualquier equipo de la red, constituyendo esto un riesgo de seguridad para la información del cliente.

Se propone migrar todos los equipos de servidores hacia el core de la red que es el mismo datacenter, para evitar riesgos de seguridad. Y se configura la resolución de direcciones DHCP dentro en los equipos del datacenter o en un servidor en uno de los puertos mediante la tecnología DHCP relay.

El servicio DHCP no tiene que estar configurado directamente en uno de los switches de distribución, muchas redes utilizan un servidor DHCP centralizado.
En este caso, los equipos de core pueden redirigir las peticiones DHCP al servidor DHCP corporativo.

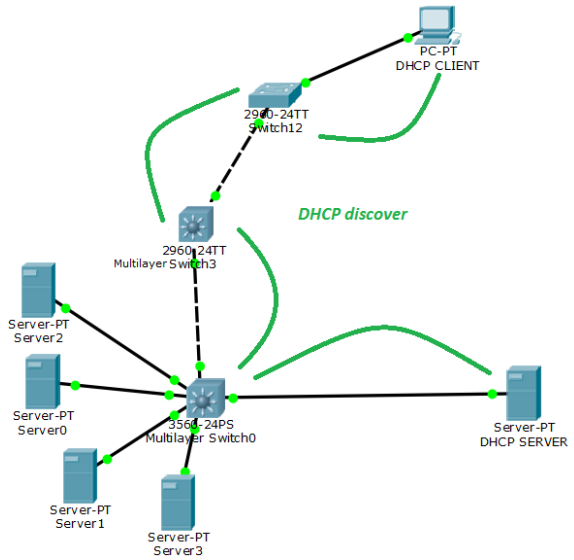



**Figura 41. Propuesta de configuración DHCP relay.**
**Fuente:** Elaboración propia.

El equipo de core debe tener una dirección IP de capa 3 que recibirá la solicitud DHCP cliente. Esta dirección puede ser un puerto del router o un SVI (interfaz virtual) y se configura ***ip helper-address***.

Cuando el switch recibe una solicitud DHCP en la forma de cliente, deja pasar el pedido como un mensaje *unicast* a la dirección IP que se especifica en el comando ***ip helper-address***. Con esta función, el switch transmite el diálogo entre el cliente y el servidor DHCP.

## IV. Mejoras a nivel de gateway en los equipos de core.

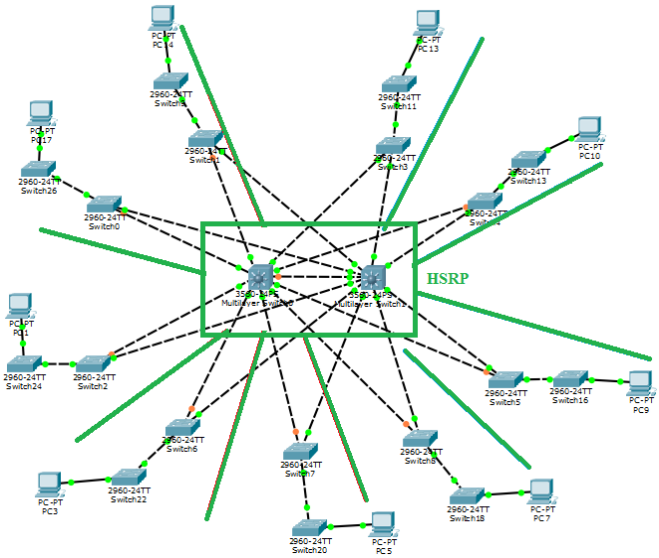



**Figura 42. Propuesta de configuración HSRP.**
**Fuente:** Elaboración propia.

Teniendo dos equipos robustos de core, es necesario habilitar ambos para dar respuesta a las peticiones de los equipos de todas las sedes. En caso de que un equipo falle no se tienen un backup para el redireccionamiento de las peticiones lo que podría causar la caída de varias sedes.

HSRP es una solución a nivel de Gateway para cuando se necesita tener un backup de protección en equipos tan esenciales como lo son el core de la red.

Una red de alta disponibilidad ofrece medios alternativos para acceder a todas las rutas de infraestructura y servidores clave en todo momento. HSRP es una de las características que se pueden configurar para proporcionar redundancia de puerta de enlace predeterminada a los hosts de red.
La optimización HSRP proporciona una conmutación por error inmediata o específica de enlace, así como un mecanismo de recuperación.

Los hosts de red se configuran con una única dirección IP de puerta de enlace predeterminada. Todos los paquetes que se destinan a otra subred se envían a la dirección IP de puerta de enlace predeterminada, que no cambia cuando se producen cambios de topología de red. Si el enrutador cuya dirección IP actúa como puerta de enlace predeterminada de los hosts de red falla, un host de red no podrá enviar paquetes a otra subred, lo que efectivamente lo desconectará del resto de la red.

HSRP utiliza una única dirección virtual para los dos equipos de core de red que funcionan como Gateway, uno de los equipos funciona como “maestro” el cual recibe todas las peticiones de los hosts, y el otro como “esclavo” el cual se encuentra en estado de standby para tomar el control en que caso de que el equipo principal falle.

## V. Otras mejoras a nivel de configuración

- Se deben configurar los puertos que van entre los equipos de acceso a los host como **PortFast**.Cuando el PC está encendido, STP tendrá que pasar por todos los estados, blocking, listening, learning, y forwarding. Con los temporizadores STP por defecto, esta transición se llevará a cabo en alrededor de 30 segundos, 15 de la listening a learning, y 15 segundos de learning a forwarding. El PC no será capaz de transmitir o recibir datos antes de que el switch de la transición al puerto de estado de forwarding. Cuando se habilita PortFast, el puerto pasará inmediatamente de blocking a forwarding. En una gran red, los ordenadores cambian de sitio a menudo, y pueden crear una gran cantidad de TCN (Topology Change Notification) si sus puertos acceso no están configurados con PortFast.

- Se debe activar seguridad en los puertos para restringir el tráfico de entrada a un puerto y limitarlo a un número de direcciones MAC permitidas que envíen tráfico al puerto. Cuando asigna direcciones MAC seguras a un puerto seguro, el puerto no reenvía el tráfico de entrada que tiene direcciones de origen fuera del grupo de direcciones definidas. Si se limita el número de direcciones MAC seguras a una y se asigna una sola dirección MAC segura, el dispositivo conectado a ese puerto tiene el ancho de banda completo del puerto.
  ***switchport port-security maximum #.***

- Habilitar un BPDU Guard en los puertos portfast para controlar la llegada de BPDU las cuales son tramas del protocolo STP para avisar sobre cambios en la topología bloqueando el puerto por seguridad tales como un cambio en la topología STP.

### 3.3.1. Síntesis de la propuesta de mejoramiento

| Problema Identificado | Solución Propuesta |
|---|---|
| Implementación de VLANs de extremo a extremo. | Implementar VLANs Locales. |
| Red completamente soportada dentro de la capa 2 del modelo OSI. | Implementar enrutamiento entre el Core, Distribución y Acceso para separar los dominios de broadcast. |
| Servidores dispersos dentro de toda la red. | Centralizar los servidores dentro del datacenter. |
| Servidor de resolución de direcciones DHCP en cada equipo de distribución. | Utilizar un único servidor DHCP centralizado en el datacenter mediante el uso de DHCP relay. |
| Gateway manualmente configurado. | Usar la tecnología HSRP para que los dos equipos de core se ocupen del tráfico en caso de un fallo en alguno de ellos. |
| **Recomendaciones** | |
| Configuración de los puertos de acceso de los equipos de acceso. | Configurar PortFast en los puertos de acceso para evitar el tiempo de transición de estados de STP. |
| Seguridad en los puertos. | Habilitar port-security para restringir el tráfico de entrada a un puerto y limitarlo a un numero de direcciones MAC permitidas |
| Filtro BPDU | Habilitar un BPDU Guard en los puertos portfast para controlar la llegada de BPDUs de STP. |

**Tabla 6. Síntesis de la propuesta de mejoramiento.**

# PARTE IV

Conclusiones

# Capítulo 4
# Conclusiones

Breve recordatorio del objetivo inicial y los objetivos específicos que se plantearon.

## 4.1. CONCLUSIONES.

- La red que presenta el cliente de telecomunicaciones es completamente obsoleta en términos de escalabilidad. No se planeó desde un principio el crecimiento de la red, afectando el rendimiento de los servicios que contiene. Si no se genera un plan de mejoramiento, como el que se presentó en la propuesta, es muy posible que con la inclusión de nuevos servicios, nuevas sedes y más usuarios finales la red deje de funcionar de manera correcta debido a las tormentas de broadcast, la transmisión de múltiples tramas y la inestabilidad en la base de datos MAC como se presenta en el la simulación propuesta (3.2.2).

- La implementación de VLANs de extremo a extremo es una práctica común debido a que están posicionadas para soportar máxima flexibilidad y movilidad de los dispositivos finales dentro de toda la red, sin embargo, su mantenimiento se vuelve complicado a medida que la red crece y cambia, además se vuelve insegura ya que se tiene acceso a todas las VLANs desde cualquier equipo intermediario representando esto un riesgo de seguridad a la información contenida en los equipos servidores del cliente, debido a esto, la implementación de VLANs locales que se presentaron en la propuesta son más fáciles de planificar ya que se establece un límite jerárquico evitando que se extiendan desde una capa de acceso a un bloque de núcleo.

- Debido a que no se hicieron mediciones de campo y tampoco fue posible manipular los equipos del cliente, no fue posible obtener resultados cuantitativos que evidencien la mejora dentro de la red, se valida el documento teniendo en cuenta la larga experiencia que posee Cisco Systems dentro del área y la documentación que ofrece dentro de su curso de certificación CCNP junto con la validación de un experto de Cisco, quien revisó el documento y estuvo de acuerdo con los criterios de la propuesta presentada. Se anexa una carta firmada por el experto, para refrendar que la propuesta de mejoramiento que se presenta en el documento es viable, posible y factible para mejorar el rendimiento de la red.

- Existen muchas ventajas sobre la implementación de redes capa 2, principalmente en costos y baja latencia. Debido al reenvío de tráfico de broadcast y ARP, se vuelven obsoletas en redes considerablemente grandes, como se muestra en el II ítem de la propuesta de mejoramiento (3.3), creando congestión y reduciendo la eficiencia de la red. Por esta razón cisco recomienda (2.2.1) disponer de equipos capa 3 para restringir el tráfico de broadcast, como las emisiones ARP y DHCP a la red local, reduciendo los niveles generales de tráfico permitiendo la administración de las redes en partes más pequeñas y restringir las emisiones solo a una subred, lo que significa que existe un límite para el tamaño de una red de capa 2. Con una red de capa 3 correctamente configurada y el conocimiento de hardware presente, se puede proveer un crecimiento infinito, por esta razón se propuso como mejor opción para mejorar el rendimiento de la red.

# BIBLIOGRAFÍA


1. **Álvares**, F., Barajas, J., Barrero, A. (2015). Comparaciones e Implementaciones de Tecnologías para las Redes Empresariales (Proyecto de Consultoría). Escuela Colombiana de Ingeniería Julio Garavito. Bogotá D.C., Colombia.

2. **CCNP** R&S ROUTE: Implementing Cisco IP Roting 300-101 Certification Exam.

3. **CCNP** R&S SWITCH: Implementing Cisco Ip Switching 300-115 Certification Exam.

4. **Contreras**, W. (2008). Propuesta para el mejoramiento de la red LAN de la compañía Danone Alquería S.A. (Tesis de Pregrado). Universidad Santo Tomás, Bogotá D.C., Colombia.

5. **Parra**, A. (2014). Propuesta de mejoramiento del desempeño de la red de telecomunicaciones para la empresa Kamilion S.A. (Tesis de Especialización). Universidad Santo Tomás, Bogotá D.C., Colombia.

6. **Sampieri**, R., Fernández, C., Baptista, L., María, P. (2006). Metodología de la investigación. México: McGraw-Hill Interamericana

7. **Szigeti**, T & Hattingh, C. (2008 c2005). End-to-End QoS Network Design. Indianapolis: Cisco Press.

8. **Tanenbaum**, A. (2003). Redes de computadoras. México: Bogotá Pearson Educación.

9. **Umasuthan**, V. (May 5, 2016). Protecting the Communications Network at Layer 2. Transmission and Distribution Conference and Exposition (T&D), 2016 IEEE/PES, 1, 5. Feb 15, 2017, De IEEE Base de datos.

# REFERENCIAS ELECTRÓNICAS


1. **Cisco** Engineers. (Sep 01, 2005). Spanning Tree PortFast BPDU Guard Enhancement. Sep, 2016, de Cisco System Sitio web: <http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10586-65.html>

2. **Cisco** Engineers. (Oct 12, 2005). Dynamically Configuring DHCP Server Options. Oct, 2016, de Cisco System Sitio web: <http://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/22920-dhcp-ser.html>

3. **Diane** Teare, Rick Graziani, Bob Vachon. (Feb 3, 2015). OSPF Implementation. Oct, 2017, de Cisco Press Sitio web :<http://www.ciscopress.com/articles/article.asp?p=2294214>

4. **Edorta,** E. (Jun 20, 2012). Tráfico broadcast. Feb, 2017, de Ciberseguridad Industrial y protección de Industria 4.0. Sitio web: <https://enredandoconredes.com/2012/06/20/trafico-broadcast/>

5. **Richard** Froom, Erum Frahim. (Jun 4, 2015). Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: Campus Network Architecture. Aug, 2016, de Cisco Press Sitio web: <http://www.ciscopress.com/articles/article.asp?p=2348266&seqNum=2>

6. **Richard** Froom, Erum Frahim. (Jun 1, 2015). Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: Network Design Fundamentals. Nov, 2016, de Cisco Press Sitio web: <http://www.ciscopress.com/articles/article.asp?p=2348265>

# Anexos

*A continuación se presenta la carta de validación del documento firmada por un experto de en redes de CISCO con el objetivo de refrendar la propuesta que se presenta en el documento.*

*Se anexa el Currículum Vítae del experto, los documentos que hacen parte a los antecedentes estudiados de la propuesta y la carta de solicitud de jurado en la carpeta de Anexos.*

ANEXO 1
CARTA DE VALIDACIÓN DE DOCUMENTO

Señor: Oscar Andrés Espinosa Erazo

Presente

Asunto: VALIDACIÓN DE DOCUMENTO A TRAVÉS DE JUICIO DE EXPERTO

Me es muy grato comunicarme con usted para expresarle mis saludos y así mismo, hacer de su conocimiento que siendo estudiante del programa de Ingeniería de Telecomunicaciones de la Universidad Santo Tomás, con sede en la ciudad de Bogotá D.C. requiero validación del documento es el cual se realiza una propuesta de mejoramiento a la red de un cliente de telecomunicaciones y con el cual optaré al título de en Ingeniero de Telecomunicaciones.

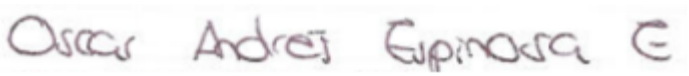
El título nombre de mi proyecto es: MEJORAMIENTO DEL RENDIMIENTO DE LA RED DE UN CLIENTE APLICANDO LAS POLITICAS DE DISEÑO DE CISCO SYSTEM, y siendo importante contar con la aprobación de un experto en el tema para refrendar la propuesta, he considerado conveniente recurrir a usted, ante su connotada experiencia y conocimientos en el campo.

El documento para validación se le hace llegar para revisión.

Expresándole mi más sincero respeto y consideración, agradezco la atención de dispense a la presente.

Atentamente.

Jorge Alberto Beleño Gómez
Estudiante de la Universidad Santo Tomás



_____
FIRMA

Certifico que la información contenida en el documento es coherente y corresponden a los parámetros de diseño y configuración más adecuados para mejorar el rendimiento de la red del cliente de telecomunicaciones que allí se presenta.