PROYECTO DE REINGENIERIA DE LA INFRAESTRUCTURA DE LA RED LAN DE SYC S.A.

SERGIO ANDRES ESPINOSA SILVA

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA DE INGENIERÍA Y ADMINISTRACIÓN

FACULTAD DE INGENIERÍA ELECTRÓNICA

BUCARAMANGA

2008

PROYECTO DE REINGENIERIA DE LA INFRAESTRUCTURA DE LA RED LAN DE SYC S.A.

SERGIO ANDRES ESPINOSA SILVA

Trabajo de grado para optar al título de Ingeniero Electrónico

Director del proyecto
ING. JHON JAIRO PADILLA

Director Empresarial
ING. JUAN CARLOS GÓMEZ
Jefe de Comunicaciones de
Sistemas y Computadores S.A.

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA Y ADMINISTRACIÓN
FACULTAD DE INGENIERÍA ELECTRÓNICA
BUCARAMANGA
2008

AGRADECIMIENTOS

A Dios nuestro señor por la oportunidad que hemos tenido de aprender, mejorar y de crecer junto a personas tan especiales para nosotros.

A mis padres por brindarnos un hogar cálido y enseñarnos que la dedicación y el esfuerzo son el camino para lograr objetivos.

A mis hermanos y hermanas, por estar siempre ahí, en los buenos y en los malos momentos.

A mi Director de Tesis, el Ing. Jhon Jairo Padilla por su generosidad al brindarme la oportunidad de recurrir a su capacidad y experiencia en un marco de confianza, afecto y amistad, fundamentales para la culminación de este trabajo.

A Sistemas y Computadores S.A por la oportunidad y la experiencia alcanzada con la realización de este proyecto.

Al Ing. Juan Carlos Gómez, por sus sabios consejos y asesoría para la orientación y realización de esta proyecto.

Al Ing. José Euclides Vera, por sus valiosas sugerencias y la oportunidad de trabajar en el desarrollo de este trabajo.

Y a todas aquellas personas que de una u otra forma, colaboraron o participaron en la realización de este proyecto, hago extensivo mi más sincero agradecimiento.

DEDICATORIA

A mis Padres por estar ahí cuando más los necesito; por su apoyo, ayuda y constante cooperación.

A mi primo que en paz descanse, porque experiencias como esas son las que dejan grandes enseñanzas.

TABLA DE CONTENIDO

1 OBJETIVOS 15

1.1 OBJETIVO GENERAL 15
1.2 OBJETIVOS ESPECÍFICOS 15

2 MARCO TEORICO 16

2.1 INTRODUCCION 16
2.2 REDES LAN. 17
2.3 DISPOSITIVOS DE INTERCONEXION 18
2.3.1 Dispositivos de red 19
2.4 ETHERNET 20
2.4.1 Tecnología y velocidad de ETHERNET 22
2.5 AGREGACION DE FLUJOS 25
2.6 CARACTERISTICAS DE *SWITCHES* DE UNA LAN 26
2.6.1 Protocolo Spanning-Tree 26
2.6.2 Operación de protocolo Spanning-Tree 29
2.7 REDES DE AREA LOCAL VIRTUALES (VLAN) 31
2.7.1 Introducción a las LAN virtuales 31
2.7.2 Aspecto Básico de las VLAN 32
2.8 PROTOCOLO TRUNKING VLAN 35
2.8.1 Enlace troncal 35
2.8.2 Protocolo de Trunking VLAN (VTP) 37
2.8.3 Operación del Protocolo de Trunking VLAN (VTP) 38

3 METODOLOGIA DEL PROYECTO 41

3.1 INTRODUCCION 41
3.2 ANÁLISIS, REQUISITOS Y DATOS 43
3.3 DISEÑO DE UNA LAN 44
3.3.1 Diseño de la red 45
3.3.2 Diseño de una red basada en switches 47
3.3.3 Capa de acceso 48
3.3.4 Descripción general de la capa de distribución 49
3.3.5 Descripción general de la capa de núcleo 50
3.3.6 Definición de segmentación y dominio de broadcast 50
3.4 TOPOLOGIA REDUNDANTES 52

4 DESARROLLO DEL PROYECTO 55

4.1 ANÁLISIS Y DIAGNOSTICO DE SISTEMA DE RED SYC S.A 55
4.1.1 Estructura inicial de la red 55
4.1.2 Estructura organizativa 61
4.1.3 Requisitos de la red 62
4.2 DISEÑO DE LA RED 62
4.2.1 Objetivos de diseño 62
4.2.2 Características del proyecto 63
4.2.3 Características del diseño de red 64
4.2.4 Topología física de la red 65
4.2.5 Descripción de la Capa de Acceso 67
4.2.6 Descripción de la Capa de distribución 68
4.2.7 Descripción de la Capa de núcleo 69
4.3 SOLUCION E IMPLEMENTACION DEL PROYECTO 70
4.3.1 Diseño e implementación capa 1 71
4.3.2 Diseño e implementación capa 2 76
4.3.3 Diseño e implementación capa 3 80

5 METODO DE CONFIGURACION DE LOS DISPOSITIVOS DE RED 89

5.1 PRACTICA 1. VERIFICACIÓN DE LA CONFIGURACIÓN POR DEFECTO DEL *SWITCH* 91
5.2 PRACTICA 2. CONFIGURACIÓN BÁSICA DE UN *SWITCH* 94
5.3 PRACTICA 3. ADMINISTRACIÓN DE LA TABLA DE DIRECCIONES MAC 96
5.4 PRACTICA 4. SELECCIÓN DEL PUENTE RAÍZ 100
5.5 PRACTICA 5. CONFIGURACIÓN VLAN ESTÁTICAS 102
5.6 PRACTICA 6. ENLACE TRONCAL CON 802.Q 104
5.7 PRACTICA 7. CONFIGURACIÓN DE SERVIDOR Y CLIENTE VTP 109
5.8 PRACTICA 8. CONFIGURACIÓN DE ENRUTAMIENTO ENTRE VLAN 111

6 ANALISIS Y RESULTADOS 115

6.1 CISCO NETWORK ASSISTANT (CNA) 116
6.2 MEDICION DE LA UTILIZACION DEL ANCHO DE BANDA DE LOS DISPOSITIVOS QUE CONFORMAN EL BACKBONE EMPRESARIAL 117

CONCLUSIONES 122

RECOMENDACIONES 124

BIBLIOGRAFIA 125

TABLA DE FIGURAS

Figura 1. Dispositivos de usuario final 18
Figura 2. Dispositivos de red 19
Figura 3. Encaminamiento con agregación de flujos 26
Figura 4. Ruta sin lazos cerrados 27
Figura 5. Operación Spanning-Tree 29
Figura 6. VLAN por ubicaciones físicas 31
Figura 7. Operación VLAN extremo a extremo 34
Figura 8. Trunking 35
Figura 9. VLAN compartidas 36
Figura 10. Enlace troncal 36
Figura 11. Encapsulamiento de trama VTP 39
Figura 12. Pasos del diseño de una red de computadores 41
Figura 13. Diseño de la topología LAN 46
Figura 14. Modelo de diseño jerárquico 47
Figura 15. Segmentación 51
Figura 16. Dominio de *broadcast* 52
Figura 17. Topología lógica SPT 53
Figura 18. Infraestructura inicial de red SYC S.A Bucaramanga 57
Figura 19. Enlaces SYC ETB 59
Figura 20. Enlaces SYC FLYCOM 59
Figura 21. Topología en estrella extendida de SYC S.A. 65
Figura 22. Diseño de Backbone 70
Figura 23. Medio de Cableado 72
Figura 24. Centro de Cableado 73
Figura 25. Centro de Cableado Principal Data Center Nivel 2 74
Figura 26. Centro de Cableado 1 Tercer piso SYC S.A 74
Figura 27. Antes y después de la auditoria 75
Figura 28. Diagrama físico de la red SYC S.A 78
Figura 29. Ejemplo de asignación de VLANs 81
Figura 30. Topología lógica de SYC S.A 88
Figura 31. Grafica de línea de conexión para prácticas de laboratorio. 90
Figura 32. Grafica de guía para las prácticas 1 y 2. 91
Figura 33. Conexión del *switch* al PC 91
Figura 34. Parámetros de configuración del puerto 92
Figura 35. Grafica de guía para la prácticas 3. 96
Figura 36. Grafica de guía para la prácticas 4. 100
Figura 37. Grafica de guía para la prácticas 5. 102
Figura 38. Grafica de guía para las prácticas 6 y 7. 104
Figura 39. Port-Channel 107
Figura 40. Grafica de guía para la práctica 8. 111
Figura 41. Vistas de dispositivos del CNA 115
Figura 42. Administración de dispositivo de red 117
Figura 43. Backbone Red SYC 118
Figura 44. Utilización del ancho de banda del SW A (Sw2R2CC1P3) 119

Figura 45. Utilización del ancho de banda del SW B (Sw2R2N2P1) 119
Figura 46. Utilización del ancho de banda del SW C (Sw1R2CC1P3) 120
Figura 47. Utilización del ancho de banda del SW D (Sw1R2N2P1) 120
Figura 48. Utilización del ancho de banda del SW E (Sw1R1N2P1) 121

LISTA DE TABLAS

Tabla 1. Formato de la trama ETHERNET 21
Tabla 2. Tecnologías Ethernet 24
Tabla 3. *Switches* capa 2 que conforma la infraestructura de red de SYC S.A. 77
Tabla 4. *Switches* de capa 3 82
Tabla 5. Esquema de direccionamiento para proyectos SYC S.A. 83
Tabla 6. Routers para enlaces ETB 86
Tabla 7. Routers para enlaces Flycom 86
Tabla 8. Modos de comando de *switch* CISCO 90
Tabla 9. Tabla de configuración de la practica 3. 96
Tabla 10. Tabla de configuración de la practica 4. 100
Tabla 11. Tabla de configuración de la practica 5. 102
Tabla 12. Tabla de configuración de la práctica 6 y 7. 104
Tabla 13. Tabla de configuración de la practica 8. 111

TABLA DE ANEXOS

Anexo A. Cisco Catalyst 2960G-24TC……..…..127
Anexo B. Cisco Catalyst 3560G-24TS…… ……...130
Anexo C. TIA/EIA – 568 A-B……....133
Anexo D. RFC 1918……...……..…..140

RESUMEN GENERAL DE TRABAJO DE GRADO

TITULO: PROYECTO DE REINGENIERIA DE LA INFRAESTRUCTURA DE RED LAN DE SYC S.A.

AUTORES: Sergio Andrés Espinosa Silva

FACULTAD: Facultad de Ingeniería Electrónica

DIRECTOR: Ing. John Jairo Padilla

RESUMEN

En los últimos años ha surgido una nueva tendencia en el desarrollo de las organizaciones, la cual ha sido el resultado de cambios importantes en el entorno interno de las empresas. La reingeniería define la pauta para cambios nuevos en la forma de operar de las organizaciones. El siguiente proyecto nace de la necesidad que tenia la empresa Sistemas y Computadores S.A de implementar una reingeniería a su infraestructura de red LAN.

Este proyecto analiza una red existente con el fin de identificar los respectivos fallos que justifican el estudio, la implementación y ejecución de un re-diseño de la red LAN empresarial. La empresa desarrolla la idea de actualización de tecnología de equipos de red, donde se efectúa la configuración correspondiente al diseño planificado y se implementan las etapas necesarias y especificas de una reingeniería de red LAN.

El desarrollo del proyecto empieza analizando los objetivos y características del diseño de red empresarial, para esto se investiga acerca de la estructura inicial de la red, la estructura organizativa y de los requisitos de red de la empresa. Se tienen en cuenta las características de diseño y se plantea una red *switcheada*, con redundancia, donde sobresalen las tres capas de diseño del modelo jerárquico de un diseño de red LAN, las cuales son capa de acceso, capa de distribución y capa de núcleo. La implementación del proyecto se hace siguiendo el orden de las tres primeras capas del modelo OSI las cuales son capa física, capa de enlace y capa de red.

El proyecto da soluciones a los problemas planteados en el análisis de la estructura inicial de red.

PALABRAS CLAVES: Red LAN, diseño de redes LAN, redes de datos, telemática, redes LAN de alta velocidad, Telecomunicaciones.

RESUMEN GENERAL DE TRABAJO DE GRADO

TITULO: PROYECTO DE REINGENIERIA DE LA INFRAESTRUCTURA DE RED LAN DE SYC S.A.

AUTORES: Sergio Andrés Espinosa Silva

FACULTAD: Facultad de Ingeniería Electrónica

DIRECTOR: Ing. John Jairo Padilla

RESUMEN

In recent years there has emerged a new trend in the development of organizations, which has been the result of major changes in the internal environment of enterprises. The reengineering sets the tone for new changes for the operation of the organizations. The following project born of necessity that the company Sistemas y Computadores S.A had to implement a reengineering of their LAN infrastructure.

The following project examines an existing network in order to identify the respective failures justifying the study, implementation and execution of a re-design of his LAN network. The company develops the idea of updating network equipment, whish the configuration for the planned design and implements is necessary for develop of the specific stages of a re-engineering LAN.

The development of the project begins with the analysis of the objectives and characteristics of network design, so for this is an investigation regarding for the initial structure of the network, the organizational structure and requirements for the corporate network. It takes into account the design features and it poses a *switch* network, with redundancy, which stand three layers of the hierarchical design model for the LAN, which are access layer, layer distribution and core layer. Also the implementation of the project is done in the order of the first three layers of the OSI model which are physical layer, link layer and the network layer.

The project provides solutions to problems raised in the analysis of the structure's original network.

PALABRAS CLAVES: Network LAN, LAN network design, data networks, Telematics, LAN high-speed, Telecommunications.

INTRODUCCIÓN

A medida que ha ido creciendo, la empresa SYC S.A ha sentido la necesidad de proyectarse y expandirse en los negocios con el fin de hacerse más productiva y mantenerse en el mercado. En este caso una de las principales necesidades que han surgido, es mejorar su infraestructura de red para el uso de los recursos para manejo de información.

A raíz de los problemas presentados con la infraestructura actual, tales como congestión en ciertos servicios de la red en algún momento del día, la perdida de conectividad entre ciertas sedes, la falta de administración de direcciones de red y servicios, etc. se propuso un proyecto orientado al análisis, diseño, implementación, operación y supervisión de sistemas para el manejo adecuado de la infraestructura de red al interior de la organización. Este proyecto se describe en el presente documento como trabajo de grado en la Facultad de Ingeniería Electrónica de la Universidad Pontificia Bolivariana bajo la supervisión conjunta de SYC S.A y el grupo de investigación de Telecomunicaciones (GITEL) de la UPB Bucaramanga.

El proyecto de reingeniería de la infraestructura de red de SYC S.A permite actualizar y proyectar la infraestructura de red de la organización a fin de cumplir con las metas estratégicas planteadas para tener una mayor competitividad y proponer las soluciones a los problemas presentados debido al crecimiento de las empresa y otros factores que impiden la alta disponibilidad en la red.

Uno de los principales objetivos del proyecto busca actualizar la plataforma tecnológica de los equipos que conforman la red de área local de la empresa Sistemas y Computadores S.A., para así poder aumentar la velocidad de conexión de 100 Mbps a 1000 Mbps y con esto unificar la infraestructura de red a nivel de fabricantes, versiones de software y capacidades de los equipos. En este caso el fabricante es *CISCO SYSTEMS*, que produce los dispositivos de red conocidos

como *Switches catalyst* 2960G de la serie 2900G (ver Anexo A) con los cuales se puede aumentar la velocidad de los enlaces hasta 1000 Mbps. Con base en la infraestructura descrita anteriormente, se construye una red sobre una base unificada. Esto permite también un sistema de configuración, monitoreo y gestión en línea para la administración de la red.

Este proyecto de tesis está organizado de la siguiente manera:
En el capítulo 1 se plantea los objetivos generales y específicos del proyecto de tesis; en el capítulo 2 se define los conceptos de interconexiones de red que se tienen en cuenta para el desarrollo del proyecto; seguidamente en el capítulo 3 se describe la metodología del proyecto, que explica las características que se tienen en cuenta en el diseño de una red; en el capítulo 4 se desarrolla el proyecto implementando los diseños de capa física, capa de enlace y capa de red. Finalmente en el capítulo 5 se explican los métodos de configuración de los equipos de red y el capitulo 6 análisis y resultados, que muestra el rendimiento de la red LAN. Por último se presentan las recomendaciones y conclusiones.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Realizar la reingeniería de la infraestructura de red de la empresa Sistemas y Computadores S.A., garantizando la disponibilidad de los servicios que presta actualmente y generando el menor impacto posible para el sistema.

1.2 OBJETIVOS ESPECÍFICOS

- Analizar el estado actual de la red de la empresa
- Determinar las soluciones a los problemas encontrados
- Re-diseñar la red con base en las soluciones planteadas
- Efectuar el cambio físico de la infraestructura de la red por equipos de última tecnología.
- Establecer para cada proyecto y área de la empresa un espacio independiente completamente definido con unas políticas claras para el manejo de acceso a la información.
- Garantizar la fluidez entre los diferentes miembros de un grupo de trabajo (VLAN) de una manera ágil y con todas las garantías de velocidad y buen ancho de banda.
- Garantizar la independencia del tráfico entre todos los segmentos de red (VLANs).
- Realizar un diseño que permita la escalabilidad de red hacia el futuro.
- Instalar un sistema de configuración, monitoreo y gestión en línea para el control de la red.

2 MARCO TEORICO

La siguiente sección busca explicar los principales conceptos de red de computadores e interconexión de redes que son necesarios para desarrollar el presente proyecto. La terminología utilizada en el proyecto está basada en la terminología usada por el fabricante CISCO SYSTEMS, ya que el uso de sus productos y servicios son utilizados por la empresa Sistemas y Computadores S.A. Además, esta terminología se emplea en los cursos de capacitación y certificación tales como el CCNA[1], realizados por el autor del siguiente documento.

2.1 INTRODUCCION

Las redes de datos se desarrollaron como consecuencia de aplicaciones comerciales diseñadas para comunicar los computadores entre sí. Antes no existía una manera eficaz de compartir datos entre varios computadores y se utilizaban disquetes para compartirlos, lo cual no era un método eficaz ni económico para desarrollar la actividad empresarial. Se presentaban problemas cómo la duplicación de equipos informáticos y de otros recursos, ineficiencia en las comunicaciones y problemas de configuración y administración de redes.

“A mediados de la década de 1980, las tecnologías de red que habían emergido se habían creado con implementaciones de hardware y software distintas. Cada empresa dedicada a crear hardware y software para redes utilizaba sus propios estándares corporativos. Estos estándares individuales se desarrollaron como consecuencia de la competencia con otras empresas. Por lo tanto, muchas de las nuevas tecnologías no eran compatibles entre sí. Se tornó cada vez más difícil la

[1] CCNA (*Cisco Certified Network Associate*) es una certificación entregada por la compañía Cisco Systems a las personas que hayan rendido satisfactoriamente el examen correspondiente, sobre infraestructuras de red e Internet. Está orientada a los profesionales que operan equipamiento de networking.

comunicación entre redes que usaban distintas especificaciones. Esto a menudo obligaba a deshacerse de los equipos de la antigua red al implementar equipos de red nuevos.

Una de las primeras soluciones fue la creación de los estándares de Red de área local (*LAN - Local Area Network)*. Como los estándares LAN proporcionaban un conjunto abierto de pautas para la creación de hardware y software de red, se podrían compatibilizar los equipos provenientes de diferentes fabricantes. Esto permitía la estabilidad en la implementación de las LAN.

A medida que el uso de los computadores en las empresas aumentaba, pronto resultó obvio que incluso las LAN no eran suficientes. Lo que se necesitaba era una forma de que la información se pudiera transferir rápidamente y con eficiencia, no solamente dentro de una misma empresa sino también de una empresa a otra. La solución fue la creación de redes de área metropolitana (MAN) y redes de área amplia (WAN). Como las WAN podían conectar redes de usuarios dentro de áreas geográficas extensas, estas permitieron que las empresas se comunicaran entre sí a través de grandes distancias."[2]

2.2 REDES LAN.

"LAN son las siglas de *Local Area Network*, Red de área local. Una LAN es una red que conecta los computadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).

---

[2] *Academia de Networking de Cisco Systems*
Guía del primer año CCNA 1 y 2 pág. 41

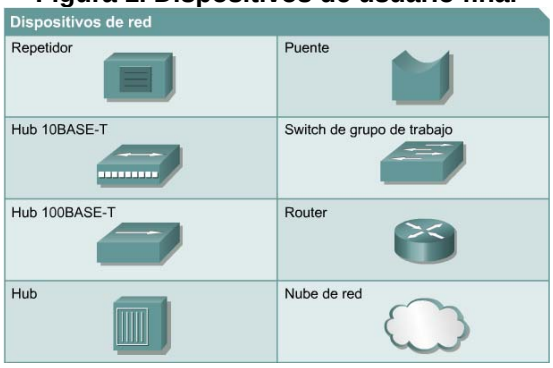
Las redes LAN se pueden conectar entre ellas a través de cables (por ejemplo líneas telefónicas, cable UTP categoría 5 o 6). Incluso, pueden conectarse a través de otra red que interconectan las LAN. Un sistema de redes LAN conectadas de esta forma se le conoce como una WAN, siglas del inglés de *wide-area network*, Red de área ancha.

Las estaciones de trabajo o los computadores personales en oficinas, están normalmente conectados en una red LAN, lo que permite que los usuarios envíen o reciban archivos y compartan el acceso a los archivos y a los datos."[3]

2.3 DISPOSITIVOS DE INTERCONEXION

Los equipos que se conectan de forma directa a un *segmento de red*[4] se denominan Dispositivos. Estos Dispositivos se clasifican en dos grandes grupos: Dispositivos de usuario final (ver figura 1.) y Dispositivos de red (ver figura 2.).

Figura 1. Dispositivos de usuario final



Fuente. http://curriculum.netacad.net/ Marzo 2008

[3] http://www.masadelante.com/faq-lan.htm

[4] Un segmento de red suele ser definido mediante la configuración del hardware (comúnmente por un router o *switch*) o una dirección de red específica.

Figura 2. Dispositivos de red

Fuente. http://curriculum.netacad.net/ Marzo 2008

"Los Dispositivos de usuario final incluyen los computadores, impresoras, escáneres, y demás Dispositivos que brindan servicios directamente al usuario. Los Dispositivos de red son todos aquellos que conectan entre sí a los Dispositivos de usuario final, posibilitando su intercomunicación."[5]

2.3.1 Dispositivos de red

Switches de capa 2 (*Switch Ethernet*)

Los *switches* de capa 2, son dispositivos de la capa de enlace de datos que permiten interconectar múltiples segmentos de red físicos en redes sencillas más grandes. Los *switches* conmutan el tráfico en base a las direcciones *MAC*. Cada puerto de *switch* proporciona a cada *host* el ancho de banda completo del medio.

Routers

Un *router* es un tipo de dispositivo de interconexión a Internet que transmite paquetes de datos entre redes basándose en direcciones de la capa 3 (Direcciones IP). Un *router* puede tomar decisiones acerca de la mejor ruta para la

---

[5] *Academia de Networking de Cisco Systems*
Guía del primer año CCNA 1 y 2 pág. 73

distribución de datos por internet. Trabajar en la capa 3, permite al *router* tomar decisiones basándose en las direcciones de red (direcciones IP), en lugar de las direcciones *MAC* individuales de la capa 2. Debido a su capacidad de enrutar paquetes con base en la información de la capa 3, los *routers* se han convertido en el soporte de Internet con base en la ejecución del protocolo IP. El propósito de un *router* es examinar los paquetes entrantes, elegir la mejor ruta para ellos a través de internet y después, conmutarlos al puerto de salida apropiado.

Firewalls

El término *firewall* se refiere a un programa ejecutándose en un *router* o a un servidor o un componente hardware independiente especial de una red. Un *firewall* protege los recursos de una red privada de los usuarios de otras redes. Utilizar un *firewall* es como utilizar un oficial de tráfico para garantizar que solo el tráfico valido puede entrar o salir de ciertas redes.

2.4 ETHERNET

"Ethernet es el nombre de una tecnología de redes de computadoras de área local basada en tramas de datos. Ethernet define las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI. Ethernet se refiere a las redes de área local y dispositivos bajo el estándar IEEE 802.3 que define el protocolo CSMA/CD, aunque actualmente se llama Ethernet a todas las redes cableadas que usen el formato de trama descrito en la tabla 1, aunque no tenga CSMA/CD como método de acceso al medio."[6]

[6] http://es.wikipedia.org/wiki/Ethernet

Tabla 1. Formato de la trama ETHERNET

	Trama de Ethernet						
Campo	**Preámbulo**	**SOF**	**Destino**	**Origen**	**Tipo**	**Datos**	**FCS**
Longitud	**7 bytes**	**1 byte**	**6 bytes**	**6bytes**	**2 bytes**	**46 a 1500 bytes**	**4 bytes**

Fuente. http://es.wikipedia.org/wiki/Ethernet, Marzo 2008

A continuación se describe los diferentes campos que conforman una trama Ethernet:

- Preámbulo

  Un campo de 7 bytes (56 bits) con una secuencia de bits usada para sincronizar y estabilizar el medio físico antes de iniciar la transmisión de datos. El patrón del preámbulo es:

  10101010 10101010 10101010 10101010 10101010 10101010 10101010

  Estos bits se transmiten en orden, de izquierda a derecha y en la codificación Manchester representan una forma de onda periódica.

- SOF Inicio de Trama (*Start Of Frame*)

  Campo de 1 byte (8 bits) con un patrón de 1s y 0s alternados y que termina con dos 1s consecutivos. El patrón del SOF es: 10101011. Indica que el siguiente bit será el bit más significativo del campo de dirección MAC de destino.

  Aunque se detecte una colisión durante la emisión del preámbulo o del SOF, el emisor debe continuar enviando todos los bits de ambos hasta el fin del SOF.

- Dirección de destino

  Campo de 6 bytes (48 bits) que especifica la dirección MAC hacia la que se envía la trama. Esta dirección de destino puede ser de una estación, de un grupo *multicast* o la dirección de *broadcast* de la red. Cada estación examina este campo para determinar si debe aceptar el paquete.

- Dirección de origen

  Campo de 6 bytes (48 bits) que especifica la dirección MAC desde la que se envía la trama. La estación que deba aceptar el paquete conoce por este campo la dirección de la estación origen con la cual intercambiará datos.
- Tipo

  Campo de 2 bytes (16 bits) que identifica el protocolo de red de alto nivel asociado con el paquete o, en su defecto, la longitud del campo de datos. La capa de enlace de datos interpreta este campo.
- Datos

  Campo de 46 a 1500 Bytes de longitud. Cada Byte contiene una secuencia arbitraria de valores. El campo de datos es la información recibida del nivel de red (la carga útil).
- FCS Secuencia de Verificación de Trama (*Frame Check Sequence*)

  Campo de 32 bits (4 bytes) que contiene un valor de verificación CRC (Control de redundancia cíclica). El emisor calcula este CRC usando todo el contenido de la trama y el receptor lo re-calcula y lo compara con el recibido a fin de verificar la integridad de la trama.

2.4.1 Tecnología y velocidad de ETHERNET

"Hace ya mucho tiempo que Ethernet consiguió situarse como el principal protocolo a nivel de enlace. Ethernet 10Base2 consiguió, ya en la década de los 90s, una gran aceptación en el sector. Hoy por hoy, 10Base2 se considera como una "tecnología de legado" respecto a 100BaseT. Hoy los fabricantes ya desarrollaron adaptadores capaces de trabajar tanto con la tecnología 10baseT como la 100BaseT y 1000BaseT, ayudando a una mejor adaptación y transición."[7]

Las tecnologías Ethernet que existen se diferencian en estos conceptos:

Velocidad de transmisión

- Velocidad a la que transmite la tecnología.

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

Tipo de cable

- Tecnología del nivel físico que usa la tecnología.

Longitud máxima

- Distancia máxima que puede haber entre dos nodos adyacentes (sin estaciones repetidoras).

Topología

- Determina la forma física de la red. Bus si se usan conectores T (hoy sólo usados con las tecnologías más antiguas) y estrella si se usan hubs (estrella de difusión) o *switches* (estrella conmutada).

Tabla 2. Tecnologías Ethernet

Tecnologías Ethernet

Tecnología	Velocidad de transmisión	Tipo de cable	Distancia máxima	Topología
10Base2	10 Mbps	Coaxial	185 m	Bus (Conector T)
10BaseT	10 Mbps	Par Trenzado	100 m	Estrella (Hub o *Switch*)
10BaseF	10 Mbps	Fibra óptica	2000 m	Estrella (Hub o *Switch*)
100BaseT4	100Mbps	Par Trenzado (categoría 3UTP)	100 m	Estrella. Half Duplex(hub) y Full Duplex(*switch*)
100BaseTX	100Mbps	Par Trenzado (categoría 5UTP)	100 m	Estrella. Half Duplex(hub) y Full Duplex(*switch*)
100BaseFX	100Mbps	Fibra óptica	2000 m	No permite el uso de hubs
1000BaseT	1000Mbps	4 pares trenzado (categoría 5UTP)	100 m	Estrella. Full Duplex (*switch*)
1000BaseSX	1000Mbps	Fibra óptica (multimodo)	550 m	Estrella. Full Duplex (*switch*)
1000BaseLX	1000Mbps	Fibra óptica (monomodo)	5000 m	Estrella. Full Duplex (*switch*)

Fuente. http://es.wikipedia.org/wiki/Ethernet**, Marzo 2008**

2.5 AGREGACION DE FLUJOS

"Un protocolo es un conjunto de reglas que determina cómo se comunican los computadores entre sí a través de las redes. Los computadores se comunican intercambiando mensajes de datos. Para aceptar y actuar sobre estos mensajes, los computadores deben contar con definiciones de cómo interpretar el mensaje. Se conocen ejemplos como la conexión a una máquina remota, mensajes de correo electrónico y archivos que se transmiten en la red.

Un protocolo describe lo siguiente:

- El formato al cual el mensaje se debe ajustar.
- La manera en que los computadores intercambian un mensaje dentro del contexto de una actividad en particular." [8]

Un protocolo enrutado permite que un *router* envíe datos entre nodos de diferentes redes. Para que un protocolo sea enrutable, debe admitir la capacidad de asignar a cada dispositivo individual un número de red y uno de Host. Protocolos, como el IP[9], requieren de una dirección completa que especifique la porción de red y la porción de Host. También necesitan de una máscara de red para poder diferenciar estos dos números. Como se observa en la Figura 3. La dirección de red se obtiene al realizar la operación "AND"[10] con la dirección y la máscara de red.

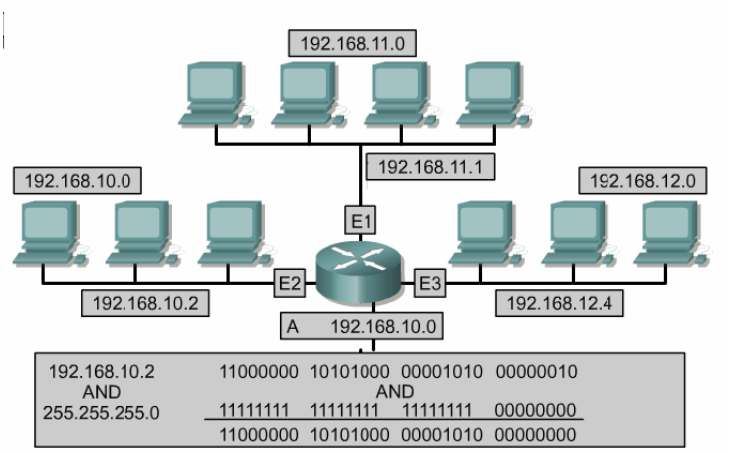
---

[8] *Academia de Networking de Cisco Systems*
Guía del primer año CCNA 1 y 2 pág. 395

[9] El Protocolo de Internet (IP, *Internet Protocol*) es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

[10] AND, es el producto de el algebra de las operaciones lógicas (0 y 1) conocido como el "algebra de Boole".

Figura 3. Encaminamiento con agregación de flujos



Fuente. http://curriculum.netacad.net/ Marzo 2008

La razón por la que se utiliza una máscara de red es para permitir que grupos de direcciones IP secuenciales sean considerados como una sola unidad. Si no se pudiera agrupar, cada Host tendría que mapearse de forma individual para realizar el enrutamiento.

2.6 CARACTERISTICAS DE *SWITCHES* DE UNA LAN

Actualmente los diseñadores de red, se inclinan por lo *switches* y los *routers* a la hora de construir una red. Las secciones que se presentan a continuación explican los conceptos y características que se deben tener en cuenta en el uso de *switches* CISCO en una LAN y así poder aplicarlas correctamente en el diseño de una red LAN.

2.6.1 Protocolo Spanning-Tree

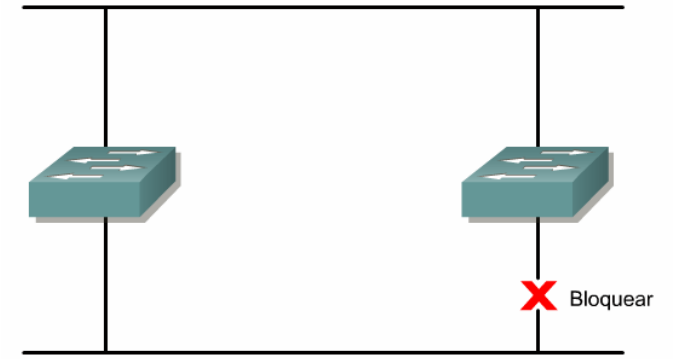
La redundancia en una red es fundamental y permite que las redes sean tolerantes a las fallas. Las topologías redundantes proporcionan protección contra

el tiempo de inactividad o a la no disponibilidad de una red. Por ejemplo, el tiempo de inactividad puede deberse a la falla de un solo enlace, puerto o dispositivo de red y por esto los ingenieros y administradores de red a menudo deben enlaces redundantes con la necesidad de tener una mayor disponibilidad de la red.

El protocolo *Spanning-Tree* IEEE 802.1d, es una herramienta poderosa que le otorga a los administradores de red la seguridad de contar con una topología redundante sin que exista el riesgo de que se produzcan problemas provocados por bucles de conmutación en una red.

Los *switches Ethernet* CISCO implementan este protocolo. *Spanning-Tree* es un algoritmo usado para desarrollar una red de ruta más corta sin lazos cerrados (ver figura 4.), para mantener una topología de red libre de bucles. Se tiene en cuenta que la ruta más corta se basa en la sumatoria de los costos de enlaces que son asignados con base en la velocidad que tiene el enlace.

Figura 4. Ruta sin lazos cerrados



Fuente. Academia de Networking de Cisco Systems Guía del prime año CNNA 3 y 4 pág. 258. Marzo 2008

El Protocolo *Spanning-Tree* establece un nodo raíz denominado puente raíz. Este protocolo desarrolla una topología que tiene, una ruta para llegar a todos los nodos de la red usando la ruta más corta. El árbol *Spanning-Tree* se origina desde el puente raíz y los enlaces redundantes que no forman parte del árbol se bloquean.

Dado que determinadas rutas están bloqueadas como se muestra en la figura 4 es posible desarrollar una topología sin bucles. Por tanto, las tramas de datos que se reciben en enlaces que están bloqueados se descartan.

El Protocolo *Spanning-Tree* requiere que los dispositivos de red intercambien mensajes para detectar los bucles cerrados y colocarlos en estado de bloqueo.

En consecuencia, los *switches* envían mensajes denominados Unidades de Datos del Protocolo Puente (*Bridge Protocol Data Unit*, BPDU) para permitir la creación de una topología lógica sin bucles. Las BPDU se siguen recibiendo en los puertos que están bloqueados. Esto garantiza que si una ruta o un dispositivo activo falla, se puede calcular un nuevo árbol de extensión.

Las BPDU contienen información que permite que los *switches* ejecuten acciones específicas como:

- Seleccionar un solo *switch* que actúe como la raíz del *Spanning-tree*.
- Calcular la ruta más corta desde sí mismo hacia el *switch* raíz
- Designar uno de los *switches* como el *switch* más cercano a la raíz, para cada segmento LAN. Este *switch* se denomina *switch* designado. El *switch* designado administra todas las comunicaciones desde la LAN hacia el puente raíz.
- Elegir uno de sus puertos como su puerto raíz, para cada *switch* que no es un *switch* raíz. Esta es la interfaz que brinda la mejor ruta hacia el *switch* raíz.
- Seleccionar puertos que forman parte del árbol de expansión. Estos puertos se denominan puertos designados. Los puertos no designados se bloquean.

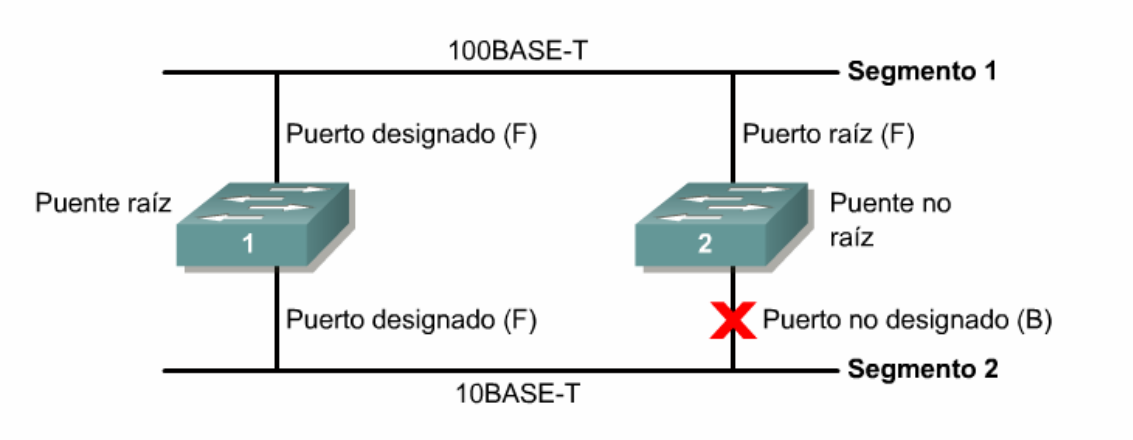
2.6.2 Operación de protocolo Spanning-Tree

Una vez que la red se ha estabilizado, se ha producido la convergencia y hay un árbol de extensión por red. Se da como resultado los siguientes elementos por cada red conmutada:

- Un puente raíz por red
- Un puerto raíz por puente que no sea raíz
- Un puerto designado por segmento
- Puertos no designados o que no se utilizan

En la figura 5 se puede observar los puertos raíz y los puertos designados que se usan para enviar tráfico de datos, también, los puertos no designados que descartan el tráfico de datos. Estos puertos se denominan puertos de bloqueo o de descarte.

Figura 5. Operación Spanning-Tree



Fuente. ***Academia de Networking de Cisco Systems Guía del primer año CCNA 3 y 4 pág. 259*** **Marzo 2008**

Selección del Puente Raíz

El puente raíz es punto principal del árbol de extensión de una red, esta es la primera decisión que toman los *switches* que conforman la infraestructura de red.

La posición del puente raíz en una red es de suma importancia ya que afecta el flujo de tráfico de pasa a través de la red.

Cuando el *switch* se enciende, se usa el algoritmo *Spanning-Tree* para identificar el puente raíz. Las BPDU son enviadas con el ID de puente (BID, *Bridge ID*). El BID se compone de una prioridad de puente que asume un valor por defecto de 32768 y la dirección MAC del *switch*. Por defecto, las BPDU's se envían cada dos segundos.

"Cuando el *switch* se enciende por primera vez, supone que es el *switch* raíz y envía las BPDU que contienen la dirección MAC del *switch* tanto en el BID raíz como emisor. Estas BPDU se consideran inferiores dado que se generan en el *switch* designado que ha perdido su enlace con el puente raíz. El *switch* designado transmite las BPDU con la información de que es el puente raíz y el puente designado a la vez. Estas BPDU contienen la dirección MAC del *switch* tanto en el BID raíz como emisor. Los BID se reciben en todos los *switches*. Cada *switch* reemplaza los BID de raíz más alta por BID de raíz más baja en las BPDU que se envían. Todos los *switches* reciben las BPDU y determinan que el *switch* que cuyo valor de BID raíz es el más bajo será el puente raíz."[11]

Es importante saber, que el administrador de red, puede establecer la prioridad del BID de un *switch* en un valor más pequeño que el del valor por defecto, lo que hace que el BID sea más pequeño y pudiendo establecer que *switch* queda como puente raíz del Spanning-Tree. Este proceso es bueno sólo implementarlo cuando se tiene un conocimiento total del flujo de tráfico en la red.

---

[11] *Academia de Networking de Cisco Systems*
Guía del primer año CCNA 3 y 4 pág. 262

2.7 REDES DE AREA LOCAL VIRTUALES (VLAN)

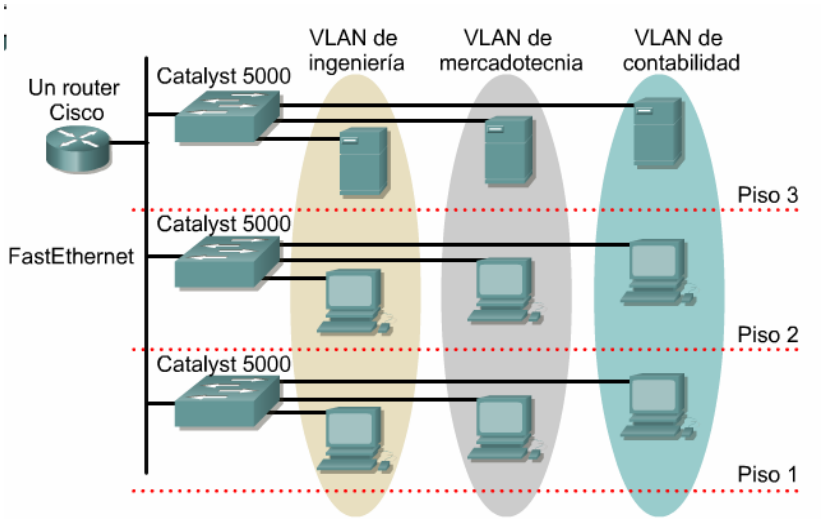
2.7.1 Introducción a las LAN virtuales

Una característica fundamental de la tecnología de conmutación *Ethernet* es la aplicación de las redes de área local virtuales (*VLAN*). Una *VLAN* es una agrupación lógica de estaciones, servicios y dispositivos de red que se encuentran ubicados en diferentes segmentos de *LAN* físico.

Las *VLAN* facilitan la administración de grupos lógicos de estaciones y servidores que se pueden comunicar como si estuviesen en el mismo segmento físico de *LAN*. También facilitan la administración de mudanzas, adiciones y cambios en los miembros de esos grupos.

Las empresas utilizan con frecuencia las *VLAN* para asegurarse de que un conjunto de usuarios en particular esta agrupado de forma lógica. Las *VLAN* segmentan de manera lógica las redes conmutadas según las funciones laborales, departamentos o equipos de proyectos, sin importar la ubicación física de los usuarios o las conexiones físicas a la red. Todas las estaciones de trabajo y servidores utilizados por un grupo de trabajo en particular pueden conformar la misma *VLAN*, sin importar la conexión física o la ubicación. (Ver figura 6)

Figura 6. VLAN por ubicaciones físicas



Fuente. Academia de Networking de Cisco Systems Guía del prime año CNNA 3 y 4 pág. 283. Marzo 2008

La configuración de las *VLAN* se logra mediante el software de configuración que implementa los *switches* CISCO. Por lo tanto, la re-configuración de una *VLAN* no requiere que los equipos de red se trasladen o conecten físicamente.

Una estación de trabajo en un grupo de *VLAN* se limita a comunicarse con los computadores, servidores u otras estaciones de trabajo que están en el mismo grupo de *VLAN*. Las *VLAN* dividen de forma lógica la red en diferentes *dominios de broadcast*, de manera tal que los paquetes sólo se conmutan entre puertos de una misma *VLAN*. Los *switches* de *LAN* operan protocolos como el *Spanning-Tree* donde se crea un arboles de expansión por cada grupo de *VLAN*.

Las *VLAN* se crean con los *switches* CISCO para brindar servicios de segmentación que tradicionalmente son proporcionados por *routers* físicos en las configuraciones de *LAN*. Así, las *VLAN* ofrecen escalabilidad, seguridad y gestión de red. Por tanto, los *routers* en las topologías de *VLAN* proporcionan filtrado de *broadcast*, seguridad y gestión de flujo de tráfico.

2.7.2 Aspecto Básico de las VLAN

En un entorno conmutado, una estación de trabajo sólo recibe tráfico dirigido a ella. Como los *switches* filtran el tráfico de red, las estaciones de trabajo en un entorno conmutado envían y reciben datos utilizando el ancho de banda completo del medio de transmisión. Al contrario de lo que ocurre con un sistema de *hubs* compartidos, en el que sólo una estación puede transmitir a la misma vez, concluyendo así que en una red conmutada permite varias transmisiones simultáneas en un *dominio de broadcast*. Este proceso no afecta directamente a las demás estaciones dentro o fuera de un *dominio de broadcast*. Por tanto, cada VLAN debe tener una dirección única de subred (red de Capa 3) asignada a ella.

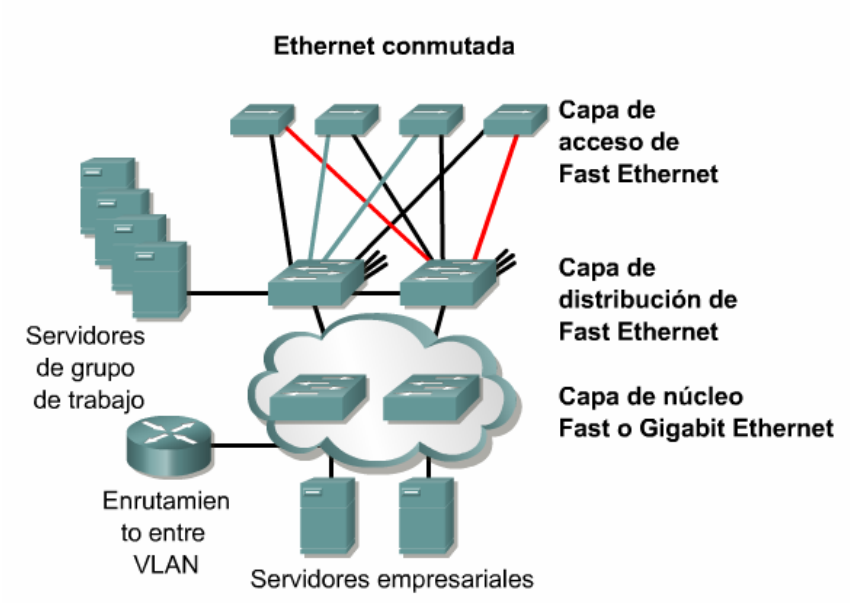
Las *VLAN* pueden existir tanto en *WAN* o internet (*VLAN* extremo a extremo), o pueden existir dentro de las fronteras geográficas de una *VLAN*.

“Una red VLAN de extremo a extremo tiene varias características:

- La asociación a las *VLAN* para los usuarios se basa en el departamento o función laboral, sin importar la ubicación de los usuarios.
- Todos los usuarios en una *VLAN* deberían tener los mismos patrones de flujo de tráfico 80/20.(Velocidad de bajada/velocidad de subida)
- Cada *VLAN* tiene un conjunto común de requisitos de seguridad para todos los miembros.

El objetivo de las *VLAN* de extremo a extremo en mantener el 80 por ciento del tráfico en la *VLAN* local. La figura 7 muestra un ejemplo de *VLAN* de extremo a extremo, donde se identifica que para construir una *VLAN*, se proporcionan puertos de *switch* para cada usuario en la capa de acceso, a su vez, cada color de unión de *switch* a *switch* representa una subred. Dado que los usuarios se reubican, cada *switch* con el tiempo contendrá miembros de todas las VLAN que puedan existir en la red.

Figura 7. Operación VLAN extremo a extremo



Fuente. Academia de Networking de Cisco Systems Guía del prime año CNNA 3 y 4 pág. 288. Marzo 2008

El protocolo enlace troncal (ISL *INTER-SWITCH*) es un protocolo propietario de Cisco que mantiene información de *VLAN* a medida que el tráfico fluye entre *switches* y *routers*. *IEEE 802.1Q* es un mecanismo de etiquetado de *VLAN* (IEEE) de estándares abiertos, en las instalaciones conmutadas. El etiquetado de tramas se utiliza para transportar información desde múltiples *VLAN* entre los *switches* de la capa de acceso y los *switches* de la capa de distribución.

De otra parte, como un criterio para definir las estaciones miembro de casa *VLAN*, y debido a que los servidores de grupos de trabajo operan de acuerdo con un modelo de cliente/servidor, es común, asignar a los usuarios la misma VLAN que el servidor que usan para maximizar el desempeño de la conmutación de Capa 2 y mantener el tráfico localizado.

Para terminar, en la Figura 7 se utiliza un *router* de capa núcleo para enrutar entre subredes también se puede hacer uso de un *switch* de capa 3. La red se diseña,

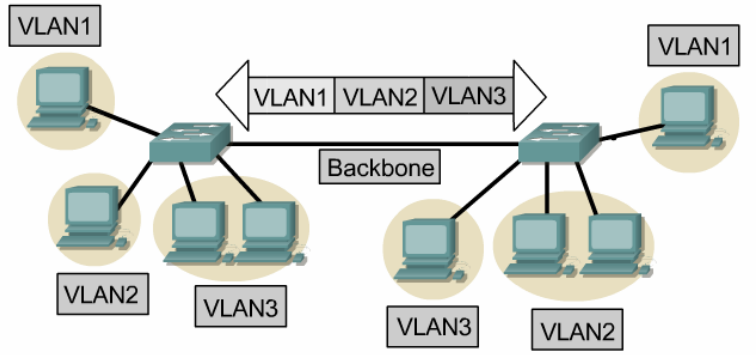
sobre la base de los patrones de flujo de tráfico, para que los miembros de una *VLAN* tengan el 80 por ciento del tráfico contenido en una ella. El 20 por ciento restante atraviesa el router a los servidores de la empresa y a la Internet o la WAN."[12]

2.8 PROTOCOLO TRUNKING VLAN

2.8.1 Enlace troncal

Un enlace troncal (*Trunking*) es una conexión física y lógica entre dos *switches* a través de la cual viaja el tráfico de red. En la figura 8 se observa un ejemplo de un enlace troncal.

Figura 8. Trunking



Fuente. http://curriculum.netacad.net/ Marzo 2008

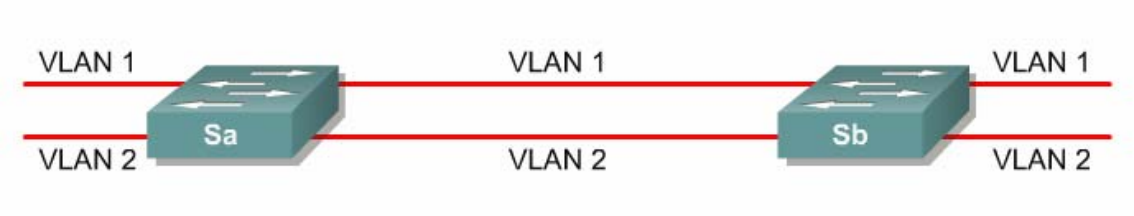
El enlace troncal es un único canal de transmisión entre dos puntos. Generalmente, los dos puntos son centros de conmutación. En una red conmutada, un enlace troncal es un enlace punto a punto que admite varias *VLAN*.

---

[12] *Academia de Networking de Cisco Systems*
Guía del primer año CCNA 3 y 4 pág. 288 y 289

El propósito de un enlace troncal es conservar los puertos cuando se crea un enlace entre dos dispositivos que implementan las *VLAN*. La Figura 9 muestra dos VLAN compartidas entre los *switches* Sa y Sb. En esta solución, cada *switch* usa dos enlaces físicos de modo que cada puerto transporta tráfico para una sola VLAN. Ésta es una forma sencilla de implementar la comunicación entre las VLAN de diferentes *switches*, pero no funciona bien a mayor escala.

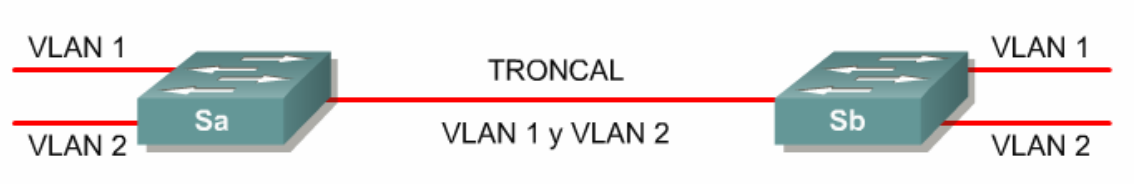
Figura 9. VLAN compartidas



Fuente. Academia de Networking de Cisco Systems Guía del prime año CNNA 3 y 4 pág. 311. Marzo 2008

Por otro lado, la adición de una tercera VLAN requiere el uso de dos puertos adicionales, uno para cada *switch* conectado. Este diseño también es ineficiente en lo que se refiere al método de compartir la carga. Además, el tráfico en algunas de las *VLAN* puede no justificar un enlace dedicado. Por tanto, una solución más adecuada es que el enlace troncal agrupa múltiples enlaces virtuales en un enlace físico (ver figura 10). Esto permite que el tráfico de varias *VLAN* viaje a través de un solo cable entre los *switches*.

Figura 10. Enlace troncal



Fuente. Academia de Networking de Cisco Systems Guía del prime año CNNA 3 y 4 pág. 311. Marzo 2008

Un enlace troncal se puede comparar con las carreteras de distribución de una autopista. Las carreteras que tienen distintos puntos de inicio y fin comparten una autopista nacional principal durante algunos kilómetros, luego se vuelven a dividir para llegar a sus destinos individuales. Este método es más económico que la construcción de una carretera entera desde el principio al fin para cada destino conocido o nuevo.

2.8.2 Protocolo de Trunking VLAN (VTP)

El protocolo de enlace troncal de *VLAN* (VTP) fue creado por Cisco para resolver los problemas operativos en una red conmutada con el uso de VLAN. VTP es un protocolo propietario de Cisco.

Piense en el ejemplo de un dominio con varios *switches* interconectados que admiten varias VLAN. Un dominio es una agrupación lógica de usuarios y recursos bajo el control de un servidor denominado Controlador de Dominio Primario (*Primary Domain Controller,* PDC). Para mantener la conectividad entre las VLAN, cada VLAN se debe configurar de forma manual en cada *switch*. A medida que la organización crece y se agregan *switches* adicionales a la red, cada nueva red debe configurarse manualmente con la información de VLAN. La asignación incorrecta de una sola VLAN puede causar dos problemas potenciales:

- Conexión cruzada entre las VLAN debido a las incongruencias de la configuración de VLAN.
- Los errores de configuración de VLAN entre entornos de medios mixtos como, por ejemplo, una LAN Ethernet y una LAN de Interfaz de Datos Distribuida por Fibra (FDDI).

Con VTP, la configuración de VLAN se mantiene unificada dentro de un dominio administrativo común. Además, VTP reduce la complejidad de la administración y el monitoreo de redes que tienen VLAN.

El rol de VTP es mantener la configuración de VLAN de manera unificada en todo un dominio administrativo de red común. VTP es un protocolo de mensajería que usa tramas de enlace troncal de Capa 2 para agregar, borrar y cambiar el nombre de las VLAN en un solo dominio. VTP también admite cambios centralizados que se comunican a todos los demás *switches* de la red.

Los mensajes de VTP se encapsulan en las tramas del protocolo de enlace Inter-*Switch* (ISL), propietario de Cisco, o IEEE 802.1Q y se envían a través de enlaces troncales a otros dispositivos. En el caso de las tramas IEEE 802.1Q, se usa un campo de 4 bytes para etiquetar la trama. Ambos formatos transportan el identificador de VLAN

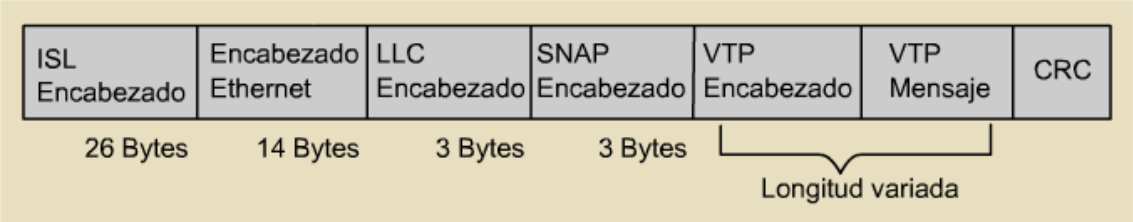
Aunque los puertos de *switch* generalmente se asignan a una sola VLAN, los puertos de enlace troncal por defecto transportan tramas desde todas las VLAN.

2.8.3 Operación del Protocolo de Trunking VLAN (VTP)

El protocolo VTP opera en un dominio compuesto de uno o más dispositivos interconectados que comparten el mismo nombre de domino, en este caso un dominio VTP. Un *switch* puede estar en un solo dominio VTP.

“Cuando se transmiten mensajes VTP a otros *switches* en la red, el mensaje VTP se encapsula en una trama de protocolo de enlace troncal como por ejemplo ISL o IEEE 802.1Q. La Figura 11 muestra el encapsulamiento genérico para VTP dentro de una trama ISL. El encabezado VTP varía según el tipo de mensaje VTP, pero por lo general siempre se encuentran los mismos cuatro elementos en todos los mensajes VTP.

Figura 11. Encapsulamiento de trama VTP



Fuente. http://curriculum.netacad.net/ Marzo 2008

- Versión de protocolo VTP, ya sea la versión 1 ó 2:
- Tipo de mensaje VTP: Indica uno de los cuatro tipos de mensajes
- Longitud del nombre de dominio de administración: Indica el tamaño del nombre que aparece a continuación
- Nombre de dominio de administración: Nombre que se configura para el dominio de administración

Los *switches* VTP operan en uno de estos tres modos:

- Servidor
- Cliente
- Transparente

Los servidores VTP pueden crear, modificar y eliminar la VLAN y los parámetros de configuración de VLAN de todo un dominio. Los servidores VTP guardan la información de la configuración VLAN en la NVRAM del *switch*. Los servidores VTP envían mensajes VTP a través de todos los puertos de enlace troncal.

Los clientes VTP no pueden crear, modificar ni eliminar la información de VLAN. Este modo es útil para los *switches* que carecen de memoria suficiente como para guardar grandes tablas de información de VLAN. El único rol de los clientes VTP es procesar los cambios de VLAN y enviar mensajes VTP desde todos los puertos troncales.

Los *switches* en modo VTP transparente envían publicaciones VTP pero ignoran la información que contiene el mensaje. Un *switch* transparente no modifica su base de datos cuando se reciben actualizaciones o envían una actualización que indica que se ha producido un cambio en el estado de la VLAN. Salvo en el caso de envío de publicaciones VTP, VTP se desactiva en un *switch* transparente.

Las VLAN que se detectan dentro de las publicaciones sirven como notificación al *switch* que indica que es posible recibir tráfico con los ID de VLAN recientemente definidos."[13]

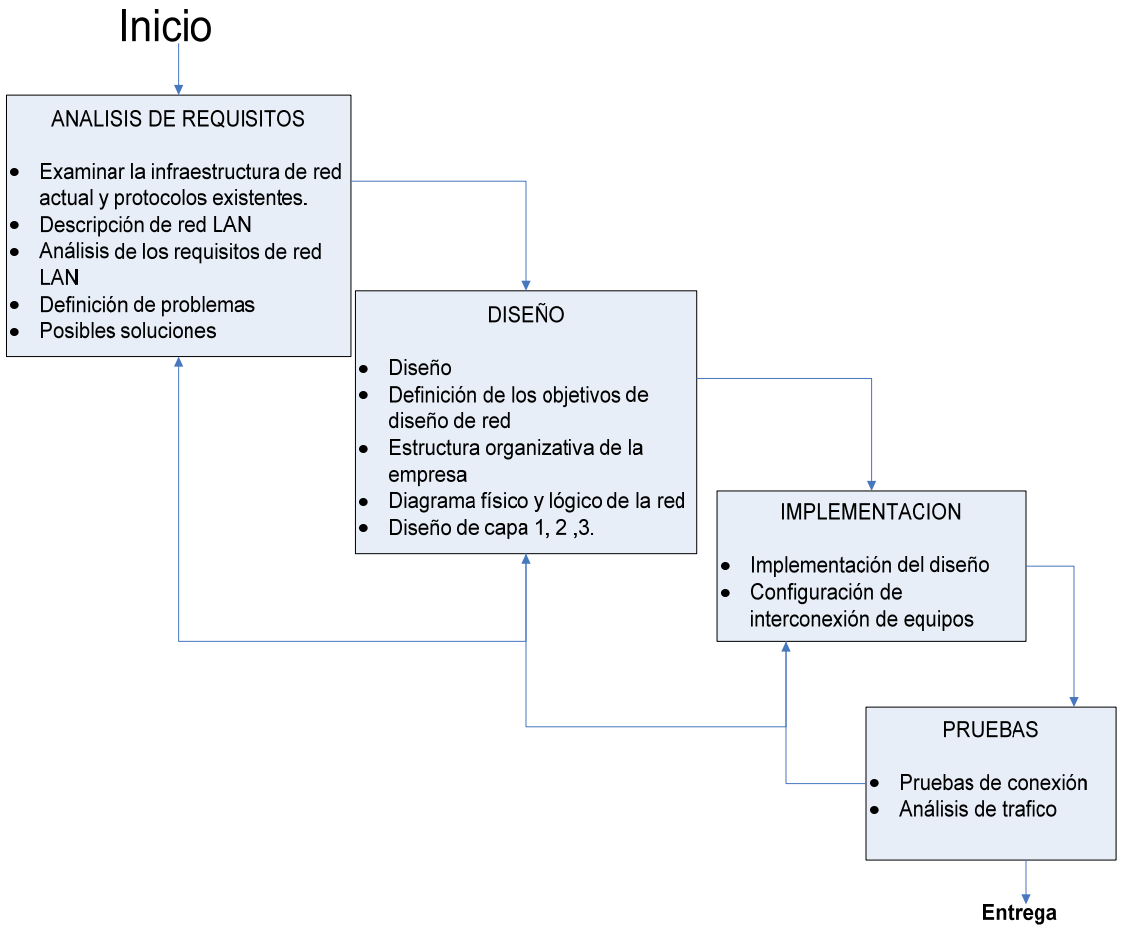
13 Academia de Networking de Cisco Systems
Guía del primer año CCNA 3 y 4 pág. 316

3 METODOLOGIA DEL PROYECTO

3.1 INTRODUCCION

Para la reingeniería de la infraestructura de red LAN de SYC S.A se deben seguir ciertos pasos típicos de un proyecto de ingeniería (ver figura 12).

Figura 12. Pasos del diseño de una red de computadores



Autor

La metodología del diseño de una LAN se describe en la figura 12. Estos pasos se definen para que una LAN sea efectiva y satisfaga las necesidades de los usuarios, donde se debe diseñar y construir de acuerdo con una serie planificada de pasos sistemáticos para así reunir los requisitos y expectativas de la red. Los pasos que se deben tener en cuenta son:

- Análisis de requisitos y datos
- Diseño de la estructura o topología de las Capas 1, 2 y 3 de la LAN
- Implementación de diseño y configuración de los dispositivos de red.
- Pruebas y análisis de tráfico.

El proyecto debe iniciar examinando la infraestructura de la red actual, haciendo una breve descripción de la red para así identificar y dar posibles soluciones a los problemas de red presentados. Al finalizar esta etapa, se deben tener claros los requisitos que puede presentar la nueva red LAN.

Luego durante la segunda etapa, se definen los objetivos del diseño de red. Estos objetivos se definen con los ingenieros de soporte de Telecomunicaciones de la empresa, que mediante entrevistas describen que servicios de red son importantes para los usuarios de la red. Es fundamental tener en cuenta la estructura organizativa de la empresa, para así diseñar un diagrama físico y lógico de red, identificando las características de diseño de capa 1, 2 y 3 del modelo OSI[14].

Por último se hace la implementación del diseño y la respectiva configuración de los equipos de red que se van a utilizar en el proyecto. Una vez la red está montada, se hacen las respectivas pruebas para determinar la funcionalidad y se realiza un análisis de tráfico para comprobar el rendimiento de la red.

[14] Modelo OSI: El modelo está compuesto por siete capas, cada una de las cuales especifica funciones de red particulares como, por ejemplo, direccionamiento, control de flujo, control de error, encapsulamiento y transferencia confiable de mensajes. La capa superior (la capa de aplicación) es la más cercana al usuario; la capa inferior (la capa física) es la más cercana a la tecnología de medios. La capa que le sigue a la capa inferior se implementa en el hardware y software, mientras que las cinco capas superiores se implementan sólo en el software. El modelo de referencia OSI se usa de forma universal como método para la enseñanza y la comprensión de la funcionalidad de la red.

3.2 Análisis, requisitos y datos

A. Recolección de información inicial

El proceso destinado a recabar información, ayuda a aclarar e identificar cualquier problema de red actual. Esta información incluye el historial de la organización y su estado actual, el crecimiento proyectado, las políticas operativas y los procedimientos de administración, los sistemas y procedimientos de oficina y los puntos de vista de las personas que utilizarán las LAN.

Deberán formularse las siguientes preguntas al reunir la información:

- ¿Quiénes son las personas que utilizarán la red?
- ¿Cuál es el nivel de capacitación de estas personas?
- ¿Cuáles son sus actitudes con respecto a las computadoras y las aplicaciones informáticas?
- ¿Cuál es el nivel de desarrollo de las políticas organizacionales documentadas?
- ¿Algunos de los datos han sido declarados críticos para el trabajo?
- ¿Algunas operaciones han sido declaradas críticas para el trabajo?
- ¿Cuáles son los protocolos que están permitidos en la red?
- ¿Sólo se soportan determinados hosts de escritorio?
- ¿Quién es responsable de las direcciones, la denominación, el diseño de topología y la configuración de las LAN?
- ¿Cuáles son los recursos humanos organizacionales, de hardware y de software?
- ¿Cómo se vinculan y comparten estos recursos actualmente?
- ¿Cuáles son los recursos financieros de los que dispone la organización?

La documentación de los requisitos permite una estimación informada de los costos y líneas temporales para la implementación de diseño de LAN. Es importante comprender los problemas de rendimiento de cualquier red.

B. Disponibilidad de la red y servicios requeridos

Por otra parte, la disponibilidad mide la utilidad de la red. A continuación, presentamos algunas de las muchas cosas que afectan la disponibilidad:

- Tasa de transferencia
- Tiempo de respuesta
- Acceso a los recursos

Cada cliente tiene una definición distinta de lo que es la disponibilidad. Por ejemplo, es posible que sea necesario transportar datos de voz y de vídeo a través de la red. Estos servicios requieren un ancho de banda mucho mayor que el que está disponible en la red o el *backbone*. Para aumentar la disponibilidad, se pueden agregar más recursos pero esto aumenta el costo de la red. Los diseños de red deben suministrar la mayor disponibilidad posible al menor costo posible.

Las necesidades del usuario de la red cambian constantemente. A medida que se introducen más aplicaciones de red basadas en voz y vídeo, la presión por aumentar el ancho de banda de la red se torna también más intensa.

Una LAN que no puede suministrar información veloz y precisa a los usuarios no tiene ninguna utilidad. Se deben tomar medidas para asegurar que se cumplan los requisitos de información de la organización y de sus trabajadores.

3.3 DISEÑO DE UNA LAN

El primer paso en el diseño de una LAN es establecer y documentar los objetivos de diseño. Estos objetivos son específicos para cada organización o situación. A continuación se describen los requisitos de la mayoría de los diseños de red:

- **“Funcionalidad:** La red debe funcionar. Es decir, debe permitir que los usuarios cumplan con sus requisitos laborales. La red debe suministrar conectividad de usuario a usuario y de usuario a aplicación con una velocidad y confiabilidad razonables.
- **Escalabilidad:** La red debe poder aumentar de tamaño. Es decir, el diseño original debe aumentar de tamaño sin que se produzcan cambios importantes en el diseño general.
- **Adaptabilidad:** La red debe diseñarse teniendo en cuenta futuras tecnologías. La red no debería incluir elementos que limiten la introducción de nuevas tecnologías a medida que éstas van apareciendo.
- **Facilidad de administración:** La red debe estar diseñada para facilitar su monitoreo y administración, con el objeto de asegurar una estabilidad en su operación.”[15]

3.3.1 Diseño de la red

El siguiente paso es decidir cuál será la topología LAN general que satisface los requisitos del usuario. La topología en estrella CSMA/CD es la configuración dominante en la industria.

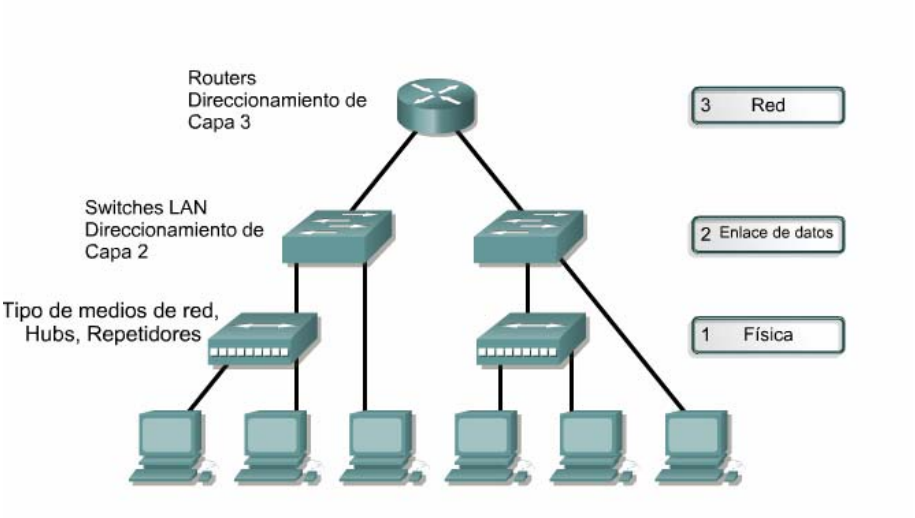
El diseño de topología LAN se puede dividir en las tres siguientes categorías únicas del modelo de referencia OSI descritas en la figura 13:

- Capa de red
- Capa de enlace de datos
- Capa física

---

[15] Academia de Networking de Cisco Systems
Guía del primer año CCNA 3 y 4 pág. 161

Figura 13. Diseño de la topología LAN



Fuente. http://curriculum.netacad.net/ Marzo 2008

El paso final en la metodología de diseño LAN es documentar la topología física y lógica de la red. La topología física de la red se refiere a la forma en que distintos componentes de LAN se conectan entre sí. El diseño lógico de la red se refiere al flujo de datos que hay dentro de una red. También se refiere a los esquemas de nombre y dirección que se utilizan en la implementación de la solución de diseño LAN.

A continuación, se presenta la documentación de diseño LAN:

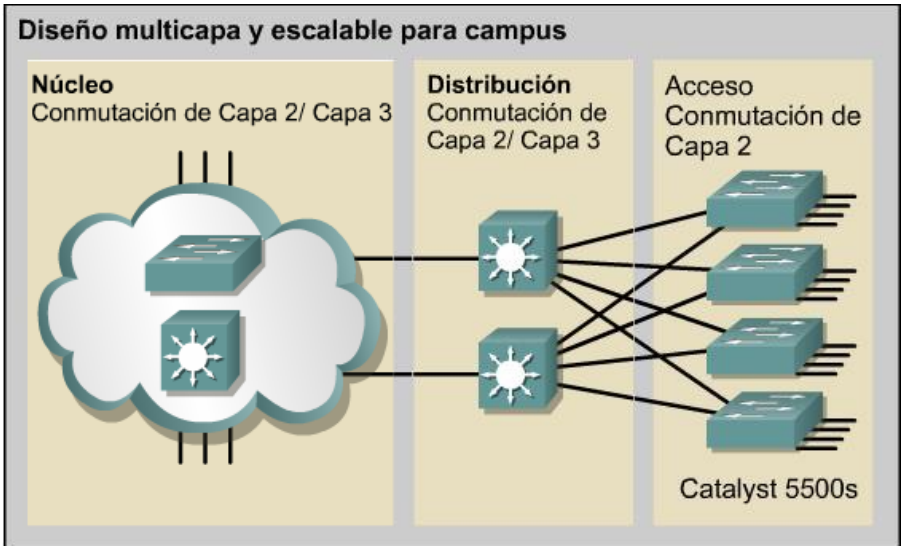
- Mapa de topología de capa OSI
- Mapa lógico de LAN
- Mapa físico de la LAN
- Planes de distribución
- Mapa lógico de VLAN
- Mapa lógico de Capa 3
- Mapas de dirección

3.3.2 Diseño de una red basada en switches

A continuación se descubrirá más en detalle los aspectos claves del diseño de la red. La construcción de una LAN que satisfaga las necesidades tanto de las organizaciones medianas como grandes tiene muchas más probabilidades de ser exitosa si se utiliza un modelo de diseño jerárquico. Un modelo de diseño jerárquico de red, se divide en tres capas para facilitar el complejo problema de diseño en problemas más pequeños y manejables. Los dispositivos de cada capa jerárquica están diseñados para aceptar el tráfico de una red y pasarlo hacia las capa superiores.

Se tiene como referencia las tres capas del modelo de diseño jerárquico descrito en la figura 14 para re diseñar una LAN más amplia para una organización:

Figura 14. Modelo de diseño jerárquico



Fuente. http://curriculum.netacad.net/ Marzo 2008

- Una capa de acceso que conecte los usuarios finales a la LAN, proporcionando a los usuarios de grupos de trabajo acceso a la red.
- Una capa de distribución que ofrezca conectividad basada en políticas entre las LAN de usuario final.

- Una capa núcleo que ofrezca la conexión más rápida que sea posible entre los distintos puntos de distribución. A la capa núcleo a veces se la denomina *backbone*.

Este modelo jerárquico se aplica a cualquier diseño de red. Es importante darse cuenta de que estas tres capas pueden existir en entidades físicas claras y definidas. Sin embargo, éste no es un requisito. Estas capas se definen para ayudar a lograr un diseño de red exitoso y representan la funcionalidad que debe existir en una red.

3.3.3 Capa de acceso

La capa de acceso es el punto de entrada para las estaciones de trabajo y los servidores de usuario a la red. En esta capa se controla la entrada de trafico a la red. En un campus LAN el dispositivo utilizado en la capa de acceso puede ser un *switch* o un *hub*.

Si se utiliza un *hub*, se comparte el ancho de banda entre todos sus usuarios. Si se utiliza un *switch*, entonces el ancho de banda es dedicado para cada usuario. Esto se debe a que el *hub* hace difusión de las tramas entrantes hacia todos los usuarios, mientras que el *switch* hace conmutación de tramas y solo las re-envía hacia el puerto del usuario destino (los demás no escuchan). Si una estación de trabajo o un servidor se conectan directamente a un puerto de *switch*, entonces el ancho de banda completo de la conexión al *switch* está disponible para la computadora conectada. Por tanto, si un *hub* se conecta a un puerto de *switch*, el ancho de banda se comparte entre todos los dispositivos conectados al *hub*.

“Las funciones de la capa de acceso también incluyen el filtrado y la microsegmentación de la capa *MAC*. El filtrado de la capa *MAC* permite a los *switches* dirigir las tramas sólo hacia el puerto de *switch* que se encuentra conectado al dispositivo destino. El *switch* crea pequeños segmentos de Capa 2

denominados microsegmentos. El *dominio de colisión*[16] puede ser tan pequeño como el equivalente a dos dispositivos. Los *switches* de Capa 2 se utilizan en la capa de acceso."[17]

Esta capa se asimila con una puerta delantera que necesita de una llave para abrir, es decir, la capa de acceso emplea listas de acceso diseñadas para impedir que usuarios no autorizados pueda ingresa a la red interna de la empresa.

3.3.4 Descripción general de la capa de distribución

"La capa de distribución de la red se encuentra entre las capas de acceso y núcleo. Ayuda a definir y separar el núcleo. El propósito de esta capa es ofrecer una definición fronteriza en la cual se puede llevar a cabo la manipulación de paquetes. Esta capa segmenta las redes en *dominios de broadcast*. Además, se pueden aplicar políticas y las listas de control de acceso pueden filtrar los paquetes. La capa de distribución aísla los problemas de red para los grupos de trabajo en los cuales se producen. La capa de distribución también evita que estos problemas afecten la capa núcleo. Los *switches* en esta capa operan en la Capa 2 y Capa 3. A continuación se presentan algunas de las funciones de la capa de distribución en una red conmutada:

- Unificación de las conexiones del armario de cableado
- Definición de dominio de *broadcast*/multicast
- Enrutamiento VLAN
- Cualquier transición de medio que deba producirse
- Seguridad"[18]

[16] dominio de colisión es un segmento Físico de una red de ordenadores donde es posible que los paquetes puedan "colisionar" (interferir) con otros. Estas colisiones se dan particularmente en el protocolo de red Ethernet.

[17] *Academia de Networking de Cisco Systems*

Guía del primer año CCNA 3 y 4 pág. 208

3.3.5 Descripción general de la capa de núcleo

"La capa núcleo es un *backbone* de conmutación de alta velocidad. Si la red no tiene un módulo de router asociado, se utiliza un router externo para la función de la Capa 3. Esta capa del diseño de red no debería realizar ninguna manipulación de paquetes. La manipulación de paquetes, como por ejemplo el filtrado de la lista de acceso, desaceleraría la conmutación de paquetes. Una infraestructura central con rutas alternadas redundantes ofrece estabilidad a la red en caso de que se produzca una única falla del dispositivo.

El núcleo se puede diseñar para utilizar la conmutación de Capa 2 o de Capa 3. Se pueden utilizar los *switches ATM o Ethernet*."[19]

El propósito de esta capa es ofrecer una estructura de transporte fiable y optimizado para reenviar el tráfico a altas velocidades. El diseño de esta capa se basa en tener varios caminos redundantes, con buen ancho de banda para que la conmutación de paquetes se haga a la máxima velocidad.

3.3.6 Definición de segmentación y dominio de broadcast

Segmentación:

Con los *switches* de capa 2 que conforman el re-diseño de la LAN, se presenta la segmentación de la red, que consiste en el proceso de dividir un único dominio de colisión en dos o más dominios de colisión de anchos de banda como lo muestra la figura 15. Los dominios de colisión más pequeños reducen la cantidad de colisiones en un segmento LAN y permiten una mayor utilización del ancho de

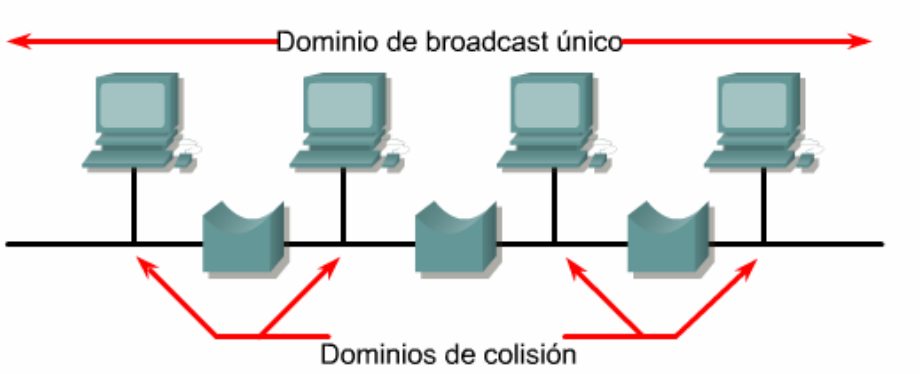
---

[18] *Academia de Networking de Cisco Systems*
Guía del primer año CCNA 3 y 4 pág. 210

[19] *Academia de Networking de Cisco Systems*
Guía del primer año CCNA 3 y 4 pág. 212

banda. El dispositivo más común de la capa 2, el *switch* LAN, determina el tamaño de los dominios de colisión de una red. Se debe tener en cuenta dos factores que afectan de forma negativa el rendimiento de una red: Las colisiones y el tamaño de los dominios de colisión. La microsegmentación de la red reduce el tamaño de los dominios de colisión y reduce las colisiones. La microsegmentación es una de las características más importantes de los *switches* LAN, cuyo objetivo es mejorar el rendimiento de un grupo de trabajo o proyecto y del *backbone*. Normalmente en la microsegmentación se utiliza la conmutación Ethernet.

Figura 15. Segmentación

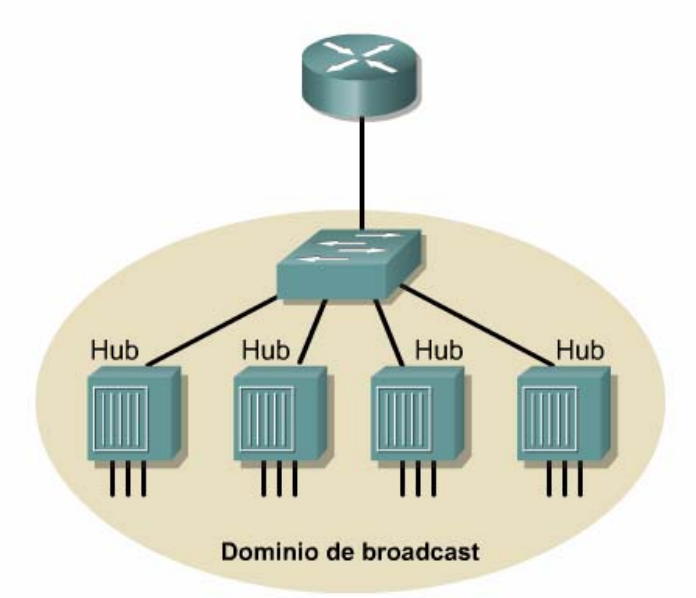


Fuente. http://curriculum.netacad.net/ Marzo 2008

Dominios de broadcast:

Un *dominio de broadcast* se refiere al conjunto de dispositivos que reciben una trama de datos de *broadcast* desde cualquier dispositivo dentro de este conjunto. Todos los hosts que reciben una trama de datos de *broadcast* deben procesarla. Este proceso consume los recursos y el ancho de banda disponible del host. Los dispositivos de Capa 2 como los puentes y *switches* reducen el tamaño de un dominio de colisión. Estos dispositivos no reducen el tamaño del dominio de *broadcast*. Los *routers* o *switches* de capa 3 reducen el tamaño del dominio de colisión y el tamaño del dominio de *broadcast* en la Capa 3, como se puede ver en la figura 16.

Figura 16. Dominio de *broadcast*



Fuente. http://curriculum.netacad.net/ Marzo 2008

3.4 TOPOLOGIA REDUNDANTES

Las topologías de red redundantes están diseñadas para garantizar que las redes continúen funcionando en presencia de puntos únicos de falla. El trabajo de los usuarios sufre menos interrupciones dado que la red continúa funcionando. Cualquier interrupción provocada por una falla debe ser lo más breve posible.

La confiabilidad aumenta gracias a la redundancia. Una red basada en *switches* o puentes presentará enlaces redundantes entre aquellos *switches* o puentes para superar la falla de un solo enlace. Estas conexiones introducen lazos cerrados en la red. Estos bucles con puentes se crean de modo que si un enlace falla, otro enlace puede hacerse cargo de la función de enviar tráfico.

Cuando un *switch* desconoce el destino del tráfico, inunda el tráfico desde todos los puertos salvo el puerto que recibió el tráfico. Las tramas de *broadcast* y

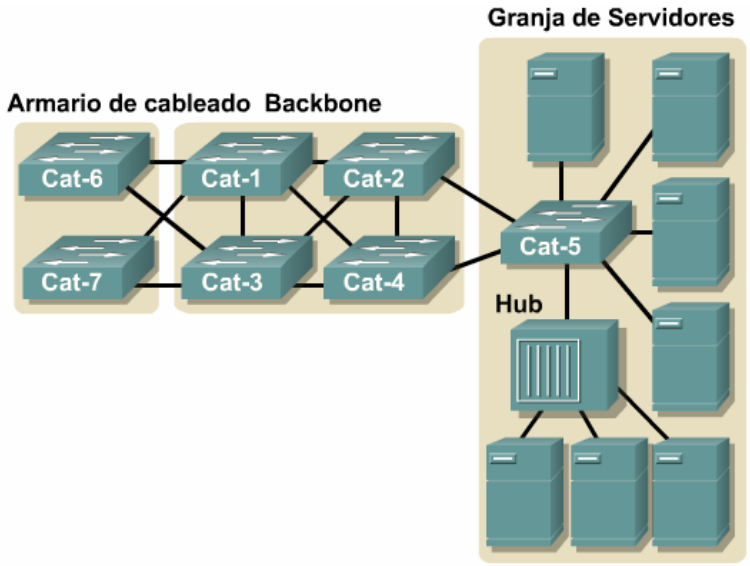
multicast también se envían por inundación desde todos los puertos, salvo el puerto que recibió el tráfico. Este tráfico puede quedar atrapado en un bucle.

En el encabezado de Capa 2, no hay ningún valor de Tiempo de vida (TTL), por lo que, si una trama se envía a una topología con bucles de *switches* de Capa 2, puede circular por el bucle indefinidamente. Esto desperdicia ancho de banda e inutiliza la red.

En la Capa 3, el TTL decrece y el paquete se descarta cuando el TTL llega a 0. Esto genera un dilema. Una topología física que contiene bucles en los caminos de los paquetes es necesaria con fines de confiabilidad, sin embargo, una red conmutada no puede tener bucles.

“La solución consiste en permitir bucles físicos, pero creando una topología lógica sin bucles. Para explicar lo anterior se tiene el ejemplo de la topología lógica de la figura 17. Según figura 17 el tráfico destinado al servidor central conectado a Cat-5 desde cualquier estación de trabajo conectada a Cat-4 viajará a través de Cat-1 y Cat-2. Esto ocurre incluso si hay una conexión física directa entre Cat-5 y Cat-4.

Figura 17. Topología lógica SPT



Fuente. http://curriculum.netacad.net/ Marzo 2008

La topología lógica sin bucles que se ha creado se denomina árbol. La topología resultante es una topología lógica en estrella o en estrella extendida. Esta topología es el árbol de extensión (*Spanning-Tree*) de la red. Se considera como un *Spanning-Tree* dado que todos los dispositivos de la red se pueden alcanzar o abarcar.

El algoritmo que se utiliza para crear esta topología lógica sin bucles es el algoritmo "*Spanning-Tree"*. Este algoritmo puede tardar un tiempo bastante prolongado para crear las tablas de enrutamiento definitivas. Por tanto, se desarrolló un nuevo algoritmo denominado algoritmo "*rapid Spanning-Tree"* para reducir el tiempo que tarda una red en calcular una topología lógica sin lazos cerrados."[20]

[20] *Academia de Networking de Cisco Systems*
Guía del primer año CCNA 3 y 4 pág. 253

4 DESARROLLO DEL PROYECTO

4.1 Análisis y diagnostico de sistema de red SYC S.A

4.1.1 Estructura inicial de la red

Para interpretar este proyecto es importante tener una comprensión básica de cómo es la infraestructura de red LAN existente. El siguiente análisis se hace con el fin de identificar los respectivos fallos que justifican el estudio e implementación de las etapas de diseño de una nueva red LAN para la organización. De igual manera, se contempla la idea de desarrollar la actualización tecnológica de equipos de red LAN para la empresa. Esto nos permitirá comprender las soluciones posibles a los problemas encontrados en la red actual de la empresa.

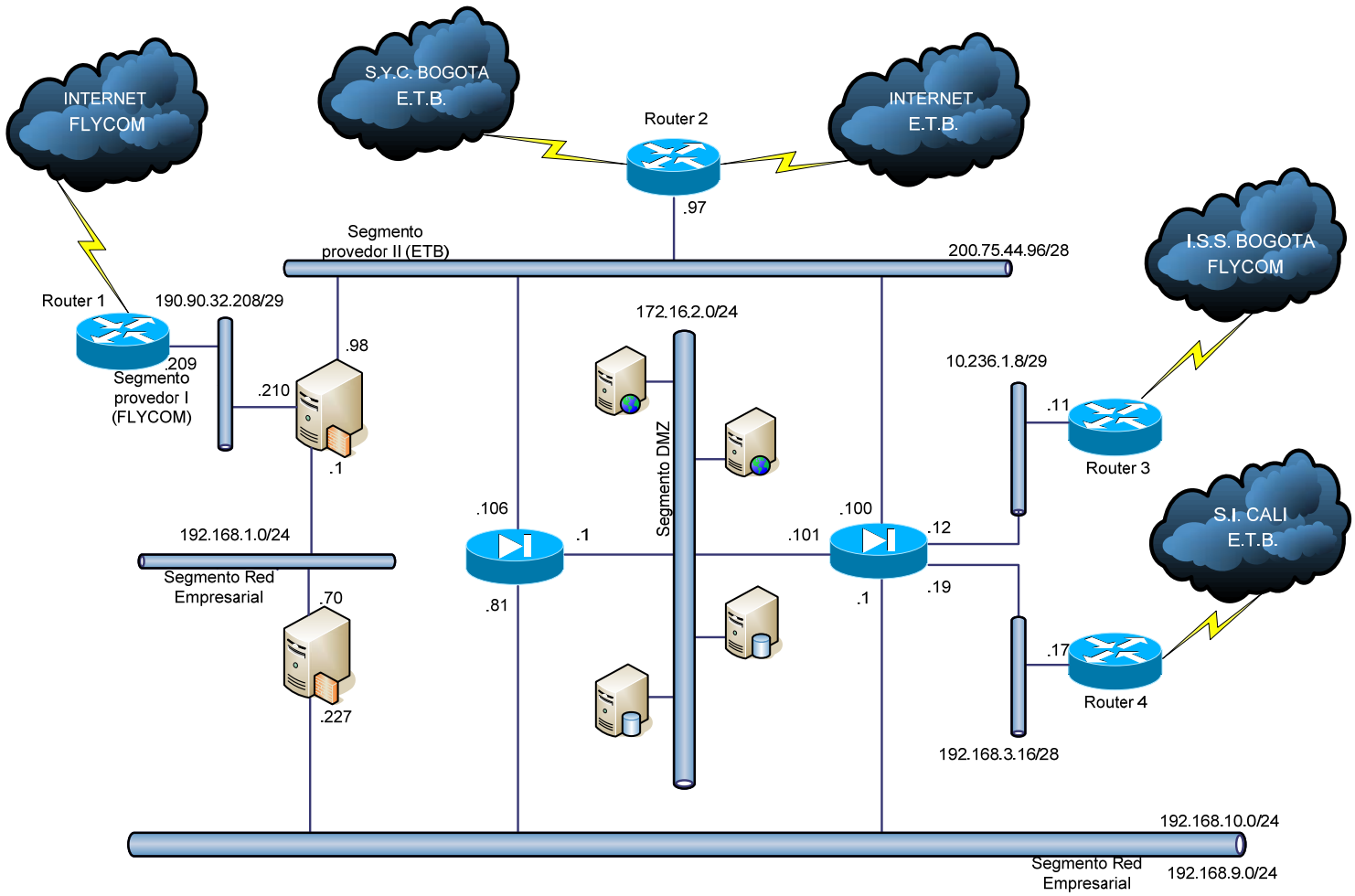
La topología lógica de red mostrada en la figura 18 corresponde a una mediana empresa llamada Sistemas y Computadores S.A. que genera soluciones informáticas integrales, prestando servicios de *outsourcing*, lo que consiste en contratar servicios externos, para desarrollar funciones específicas en diferentes campos de una organización.

A medida que la empresa fue creciendo, se vio en la necesidad de proyectarse y expandirse en los negocios con el fin de obtener más productividad y mantenerse en el mercado. Adicionalmente, su infraestructura de red empezó a presentar dificultades de tráfico que evidenciaron problemas de diseño de red que podrían llevar al colapso de la misma.

Es así como una de las principales necesidades que surgen, es la de mejorar la infraestructura de red para optimizar los recursos del manejo de información. De

esta forma, nace la idea de desarrollar un proyecto orientado al análisis, diseño, implementación, operación y supervisión de redes de comunicación, para el manejo adecuado de la infraestructura de red al interior de la organización.

Figura 18. Infraestructura inicial de red SYC S.A Bucaramanga



AUTOR

La red inicial de la empresa (figura 18) consta de dos enlaces a Internet denominados ***proveedor I (FLYCOM) y proveedor II (ETB).*** Estos enlaces que ingresan a la red por medio del router 1 y router 2 respectivamente. El tráfico de internet llega a un Proxy cuya finalidad es permitir el acceso a Internet a todos los equipos de la organización.

Además, la red también tiene tres enlaces dedicados para la interconexión de sus diferentes sedes en varias ciudades del país. Estos enlaces son contratados con los proveedores FLYCOM y ETB. Con ETB, por medio del router 2, se tiene conexión con SYC Bogotá. Y por medio del router 4 con SYC Cali. Con FLYCOM, el router 3 tiene la conexión con I.S.S Bogotá.

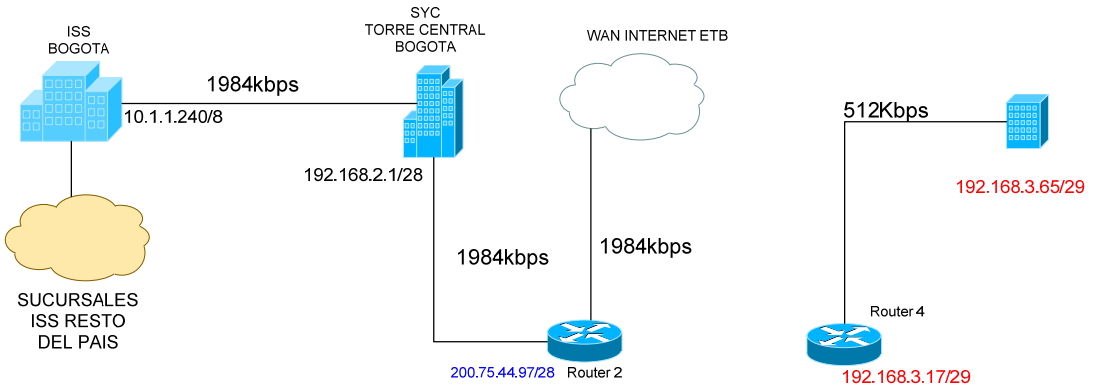
Por otro lado, en la red interna, existe el segmento denominado la DMZ, que se conoce como la red de servidores internos de la empresa. Este segmento debe ser seguro por la información que se maneja internamente. Por esto, para entrar a la DMZ existen dos *firewalls*[21] que controlan la entrada al segmento de servidores.

Adicionalmente, la red empresarial consta de tres segmentos donde más de un grupo de trabajo o proyecto de la empresa comparten la misma sub red y por tanto comparten el ancho de banda de la misma generando problemas de congestión.

En las figuras 19 y 20 se muestra la interconexión existente entre las diferentes sedes de la empresa SYC en el país.

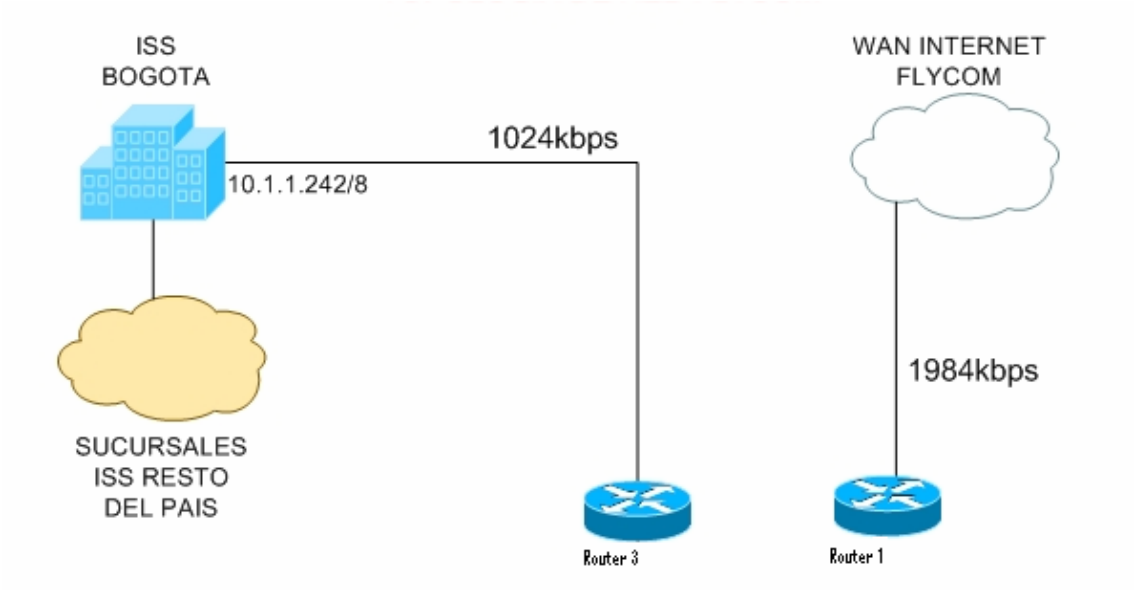
[21] Firewalls: Router o servidor de acceso, o varios routers o servidores de acceso, designados como un búfer entre cualquier red pública conectada y una red privada. El router firewall usa listas de acceso y otros métodos para garantizar la seguridad de la red privada.

Figura 19. Enlaces SYC ETB



AUTOR

Figura 20. Enlaces SYC FLYCOM



AUTOR

Al revisar la interconexión del enlace con ETB (figura 19) el router 2 tiene dos interfaces seriales: la conexión del enlace de internet y la del enlace de datos SYC Bogotá. Las dos comparten la misma entrada a la red local por la interfaz Ethernet del router. Esto evidencia uno de los problemas de diseño de red, ya que se tienen dos enlaces entrando solo por una interfaz Ethernet. Tener tráfico distinto en una misma interfaz puede generar problemas de red.

La descripción de la topología lógica (figura 18) deja al descubierto problemas de diseño de red que explican el por qué del proyecto de reingeniería. La red

llega a un punto donde por la cantidad de tráfico en un mismo segmento se cae de manera inesperada, teniendo que parar los procesos y reiniciarlos nuevamente. Al suceder esto, no se puede tener claridad de donde se origina la falla porque solo existen tres *dominios de broadcast*[22] únicos para toda la empresa. Un *dominio de broadcast* muy grande presenta demasiadas colisiones bajando el rendimiento de la red. Al tener proyectos o grupos de trabajo en un mismo segmento, el manejo de direcciones es desordenado ya que no existe un servidor DHCP[23]. No existe un sistema de administración de red y como consecuencia, se comparten las direcciones de producción del área del centro de datos, la dirección de área administrativa y la división de ingeniería causando problemas de desempeño y de asignación errada de direcciones. De esta forma, se presentan casos donde se toman direcciones que pueden estar siendo utilizadas.

Por tanto hace falta un sistema de gestión que ofrezca claridad acerca de cómo está definida la red, cuales son los puntos que se están utilizando y como es el desempeño de trafico de la red.

Por otra parte, la capacidad de la red es de 100 Mbps, y los equipos de red utilizados son *switches CISCO Catalyst 2950* de la serie 2900 (ANEXO A) con tecnología *Fast Ethernet*. Sin embargo, no existe un *backbone*[24] entre el centro de datos, el área de operación y el área administrativa de la red, donde las conexiones de red son de nivel UTP de categoría 5 con un ancho de banda 100 Mbps. Adicionalmente, en la empresa existen servidores en que su interfaz de

---

[22] *Broadcast*: Paquete de datos que se envía a todos los nodos de una red. Los *broadcast* se identifican a través de una dirección de *broadcast*.

Dominios de *broadcast*: Conjunto de todos los dispositivos que reciben tramas de *broadcast* que se originan en cualquier dispositivo del conjunto. Los dominios de *broadcast* generalmente están limitados por routers dado que los routers no envían tramas de *broadcast*.

[23] Un servidor DHCP (Dynamic Host Configuration Protocol) se utiliza para asignar direcciones IP a las computadoras de los usuarios cuando éstas arrancan.

[24] Backbone: La parte de la red que actúa como la ruta primaria para el tráfico que se origina o tiene como destino otras redes.

red es Giga bit Ethernet, lo que genera un cuello de botella en el tráfico de datos de estos equipos al pasar por los enlaces que operan a 100 Mbps.

4.1.2 Estructura organizativa

La red, como fue descrito anteriormente, pertenece a una mediana empresa llamada Sistemas y Computadores S.A, la cual es una empresa diseñada para ofrecer servicios de *Outsourcing*.

Según la misión de la empresa, "SYC es una empresa generadora de soluciones informáticas integrales, que cuenta con los mejores recursos técnicos y humanos existentes en Colombia. Tiene una experiencia de más de 25 años, donde brinda un servicio confiable, rápido y de excelente en la implementación de las últimas técnicas para el manejo de la información.
Está conformada por un equipo de más de 400 hombres y mujeres, con distintos talentos que trabajan por el desarrollo social y cultural."[25]

SYC es una empresa en crecimiento constante, que consta de varios proyectos que manejan un tráfico considerable de información dentro y fuera de la organización. A su vez, la red LAN empresarial es usada por todas las personas que conforman la empresa, donde la mayoría son ingenieros y operadores con un alto grado de experiencia en el uso de computadores y aplicaciones de servidores. Cada proyecto de la organización maneja información que es considerada crítica e importante y que no puede ser vista por toda la red o puede tener prioridad con respecto a otro tipo de información.

SYC consta con un departamento de sistemas de información. El *Data Center* de Sistemas y Computadores S.A es el que tiene la autoridad sobre el direccionamiento, diseño de la topología y la configuración de la red.

[25] http://www.syc.com.co/

4.1.3 Requisitos de la red

De acuerdo a los problemas mencionados anteriormente en el Análisis y diagnostico del sistema de red SYC S.A, la reingeniería de la infraestructura de la red LAN de SYC S.A debe presentar una red redundante con escalabilidad y políticas de seguridad establecidas. Donde cada uno de los grupos de trabajo de la empresa tendrá su espacio independiente con fluidez de tráfico y buen ancho de banda.

El re-diseño debe satisfacer las necesidades de los usuarios de red, de manera que tengan acceso en todo momento a los recursos definidos y las aplicaciones usadas. Para esto, se tiene en cuenta una red redundante y adaptable usando equipos de última tecnología que no pueda limiten la implementación de nuevas tecnologías que pudieran aparecer. Los equipos utilizados son de marca *CISCO,* marca reconocida a nivel mundial en el campo de telecomunicaciones. Los equipos a utilizarse se escogen por sus características para la implementación de este proyecto.

El rediseño de la infraestructura de red LAN tiene la siguiente filosofía:
"Una LAN que es incapaz de ofrecer a sus usuarios información puntual y precisa es de poca utilidad. Por tanto, debe dar los pasos necesarios para asegurarse de que se satisfacen los requisitos de la empresa y sus trabajadores."[26]

4.2 DISEÑO DE LA RED

4.2.1 Objetivos de diseño

Con el proyecto de la reingeniería de la infraestructura de red se desarrollará una mejor organización de las direcciones de la red interna, para obtener un

[26] *Academia de Networking de Cisco Systems Guía del primer año CCNA 3 y 4 pág. 166*

mejor rendimiento. Para esto se deben evaluar todas las necesidades que la empresa requiera, Es decir, se debe tener en cuenta cual es el ancho de banda necesario para trabajar, los segmentos en que se va a re estructurar la red y como se van a ubicar. Que equipos se deben utilizar, cuantos y que herramientas se pueden utilizar para administrar la red.

Por esto, se debe establecer un diseño para la nueva arquitectura de red que tenga todos los requisitos de la organización y de las áreas involucradas con sus respectivos requerimientos. El proyecto debe tener un plan de migración de red definiendo un cronograma de actividades, ya que la empresa tiene una producción que debe estar operando diariamente. Por lo que el cambio propuesto tiene que causar el menor daño posible y el menor impacto dentro de los proyectos de la organización.

4.2.2 Características del proyecto

Con base en el estándar a 1000 Mbps se desarrollo un re-diseño de la red donde se aprovechan las características de los dispositivos teniendo en cuenta que es de un mismo fabricante. Para la solución presentada se debe tener en cuenta que una red requiere muchas funciones para que sea confiable, escalable y fácil de administrar. Para re-diseñar este tipo de red, los diseñadores deben darse cuenta de que cada uno de los componentes principales de una red tiene requisitos de diseño específicos. Además, se deben tener en cuenta los requisitos y necesidades específicas de la red a diseñar, con el fin de mejorar el rendimiento y reducir las dificultades asociadas con el crecimiento y la evolución de la red.

El primer paso en el re-diseño de la red LAN de la organización es establecer los objetivos de diseño. Se tiene en cuenta la funcionalidad, escalabilidad, adaptabilidad y facilidad en la administración, que están descritos en la sección de *3. Metodología del proyecto.*

El re-diseño propuesto se basa en arquitecturas LAN complejas que utilizan LAN conmutadas y LAN virtuales (VLAN). Esto se debe a que para la

estructura de la red LAN se utilizan los dispositivos de red CISCO conocidos como *switches* de capa 2 y 3. Para este tipo de diseño de red empresarial se tiene presente la función y ubicación de los servidores, los temas relacionados con los dominios de colisión, temas de segmentación y la relación con los *dominios de broadcast*. Esto es para maximizar el ancho de banda y el rendimiento disponible de la LAN.

4.2.3 Características del diseño de red

Anteriormente en la sección 3. Metodología del proyecto se mencionaron características como la capas del diseño jerárquico de una red y definiciones de segmentación y *dominios de broadcast.* Una de las principales características que se deben tener en cuanta en un diseño de una red LAN es la función y ubicación de los servidores.

"Los servidores permiten que los usuarios de red se comuniquen y compartan archivos, impresoras y servicios de aplicación. Habitualmente los servidores no operan como estaciones de trabajo. Estos ejecutan sistemas operativos especializados como por ejemplo NetWare, Windows NT, UNIX y Linux. Cada servidor por lo general está dedicado a una función, por ejemplo, correo electrónico o archivos compartidos."[27]

Los servidores se clasifican en dos categorías: servidores de empresa y servidores de grupo de trabajo. El re diseño tiene incluido los servidores de empresa, que soportan a todos los usuarios de la red, ofreciendo servicios como correo electrónico. Los servidores de empresa deben estar ubicados en el diseño dentro de un armario de distribución principal, que en este caso es conocido como el segmento DMZ (ver figura. 18), descrito anteriormente. De esta forma el tráfico hacia los servidores de grupo, solo tiene que viajar hacia este segmento específico y no recorrer otras redes. Los enlaces de los

[27] *Academia de Networking de Cisco Systems Guía del primer año CCNA 3 y 4 pág. 161*

dispositivos de red deben tener asignados por lo menos 100 Mbps. En el re diseño presentado, gracias a los *switches* 2960G, tienen una conexión de 1000 Mbps.

4.2.4 Topología física de la red

La empresa ubicada en el centro empresarial Chicamocha Bucaramanga – Colombia, tiene ubicación en los tres pisos del edificio. En el primer piso se encuentra el DataCenter, que es el departamento de sistemas de información, donde están ubicados los servidores de la empresa y se administra la red LAN empresarial. En el segundo piso se encuentran los departamentos SYC Editorial e ingeniería y en el tercer piso la oficina principal de SYC S.A.

De acuerdo a los requisitos globales de la red, la topología que mejor define las necesidades de la red es una estrella extendida como se describe en la figura 21, que aparte de ser la configuración dominante en el mercado, utiliza la tecnología CSMA/CD[28] bajo el estándar Ethernet 802.3, la cual es actualmente utilizada por la empresa. La topología de la figura 21 es sacada del sistema de gestión llamado el asistente de redes de CISCO (*CISCO NETWORK ASISTANT, CNA*) que es utilizado para administrar la red de la empresarial. La figura fue adaptada en donde muestra la conexión de todos los *switches* que utiliza la empresa por medio de enlaces troncales (*Trunks*) y la ubicación de cada *switch* en los distintos pisos del edificio. También podemos ubicar las capas del diseño jerárquico que están explicadas en la 3 siguientes secciones del proyecto, donde se observan la capa de acceso que son los *switches* que dan conexión al usuario final, la capa de distribución y la capa de núcleo donde se identifican los 5 *switches* que la conforman con color blanco y el *switch* de capa 3 de color negro.

[28] Acceso múltiple con detección de portadora y detección de colisiones. Mecanismo de acceso a los medios en que los dispositivos que están listos para transmitir datos verifican primero el canal en busca de una portadora. Si no se detecta ninguna portadora durante un período de tiempo determinado, el dispositivo puede comenzar a transmitir. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que han tenido una colisión. Esta colisión retarda las transmisiones desde aquellos dispositivos durante un período de tiempo aleatorio. El acceso CSMA/CD se usa en Ethernet e IEEE 802.3.

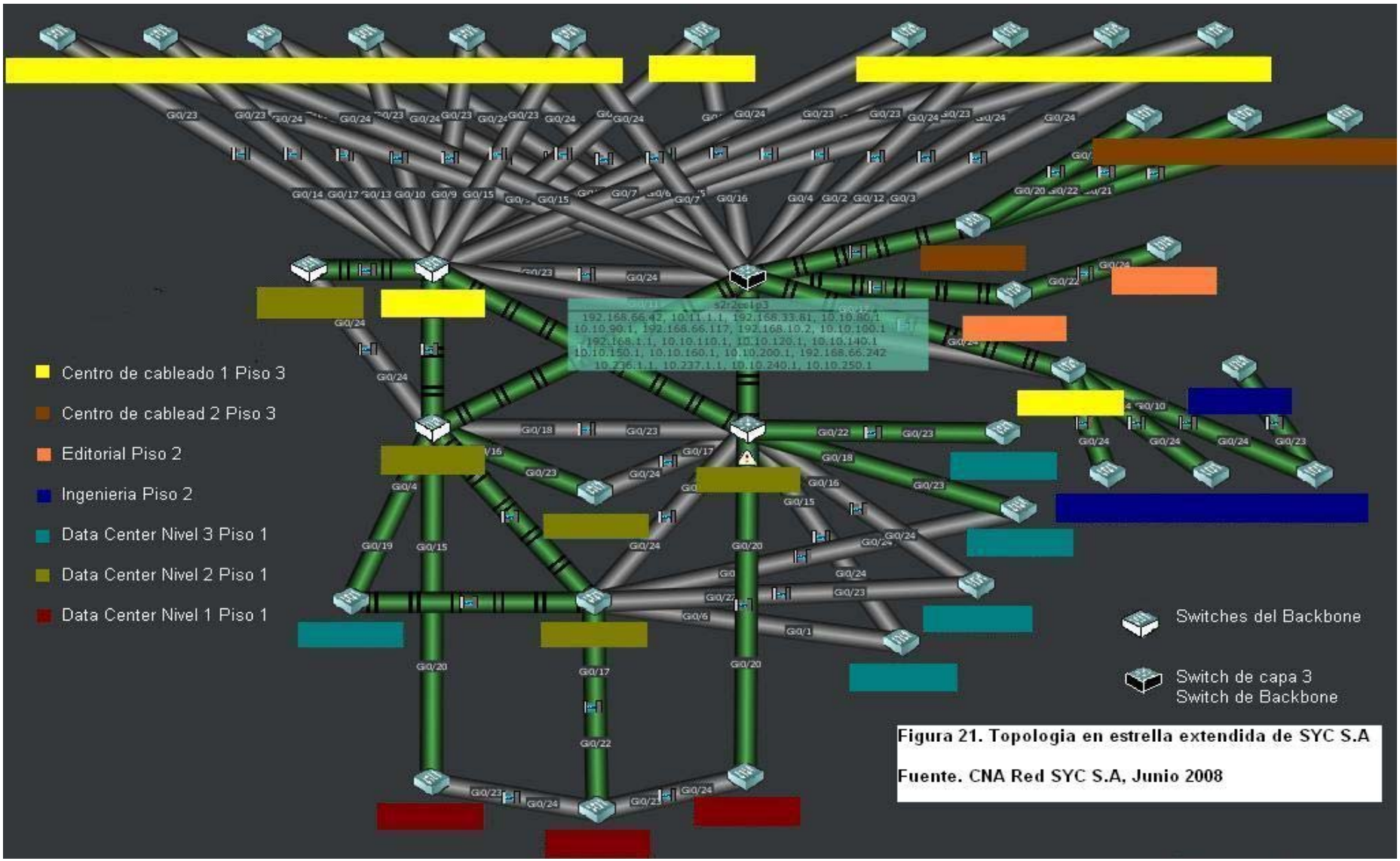


Figura 21. Topologia en estrella extendida de SYC S.A

Fuente. CNA Red SYC S.A, Junio 2008

La reingeniería de la infraestructura de red plantea dejar una dirección de sub-red para cada proyecto haciendo una comunicación por medio de VLANs y *trunks*, utilizando un *switch* de capa 3 como enrutador. Con esto vemos las piezas más importantes del diseño de una topología LAN, las cuales se dividen en tres categorías únicas del modelo de referencia OSI: la capa de red, la capa de enlace de datos y la capa física, explicadas anteriormente en la figura 16.

4.2.5 Descripción de la Capa de Acceso

La capa de acceso se conoce como el punto de entrada para las estaciones de trabajo y los servidores de usuario a la red. El dispositivo utilizado en la capa de acceso puede ser un *switch* o un *hub*.

Para la reingeniería de la infraestructura de red LAN de SYC S.A se utilizan los *switches*, para tener ancho de banda dedicado. Esto quiere decir que si una estación de trabajo o un servidor se conecta directamente a un puerto de *switch*, entonces el ancho de banda completo de la conexión al *switch* está disponible para el *host* o servidor conectado. En caso de tener un *hub* conectado a un puerto de *switch*, el ancho de banda se compartiría entre todos los dispositivos conectados al *hub*.

Anteriormente los puertos de los *switches* manejaban un ancho de banda de 100 Mbps usando tecnología *Fast Ethernet.* Con el cambio de estructura física, donde se cambiaron los equipos *switch* catalyst CISCO de un 2950 a un 2960G de la serie 2900G, el puerto subió a 1000 Mbps usando la tecnología Giga Ethernet obteniendo así un ancho de banda de 1000 Mbps.

Dos de las funciones más importantes de la capa de acceso son el filtrado y la micro segmentación de la capa MAC[29]. El funcionamiento del *switch* genera una tabla de direcciones MAC de los distintos dispositivos que están conectados en los diferentes puertos. Cuando el *switch* hace el filtrado de la

[29] MAC: Dirección de capa de enlace de datos estandarizada que se requiere para cada puerto o dispositivo que se conecta a una LAN. Otros dispositivos de la red usan estas direcciones para localizar puertos específicos en la red y para crear y actualizar tablas de enrutamiento y estructuras de datos. Las direcciones MAC tienen 6 bytes de largo y se controlan a través de la IEEE. También denominada dirección de hardware, dirección de capa MAC o dirección física.

capa MAC, permite dirigir las tramas sólo hacia el puerto de *switch* que se encuentra conectado al dispositivo destino. El *switch* también crea pequeños segmentos de Capa 2 denominados micro segmentos. Cada micro segmento es llamado un dominio de colisión[30], que puede ser tan pequeño como el equivalente a dos dispositivos.

La capa de acceso es fácilmente identificada en la figura 21, ya que son todos los *switches* que no hacen parte del núcleo o *backbone*. Estos *switches* son usados para conectar al usuario final.

4.2.6 Descripción de la Capa de distribución

La capa intermedia se conoce como la capa de distribución de la red y está entre las capas de acceso y núcleo. Los *switches* en esta capa operan en la Capa 2 y Capa 3 del modelo OSI ya que delimitan el dominio de *broadcast*, combinan el tráfico VLAN y son un punto focal para las decisiones de políticas sobre flujo de tráfico.
Este proyecto utiliza un *switch* CISCO *catalyst* 3560G de la serie 3000 (ver ANEXO B.) en la capa de distribución. Este *switch* de capa 3 tiene como propósito ofrecer una definición fronteriza en la cual se puede llevar a cabo la manipulación de paquetes. El *switch* de capa 3 segmenta las redes en *dominios de broadcast* y crea ACL's, que son las listas de control de acceso, para filtrar los paquetes y separar el tráfico de la red.

La red conmutada que se presenta en la reingeniería de la infraestructura de red de SYC S.A (ver figura 21) presenta varias funciones que se encuentran en la capa de distribución. El *switch* de capa 3 utilizado en el re-diseño separa los *dominios de broadcast*, aplica enrutamiento de VLAN, separa el tráfico de la red y brinda seguridad. En la figura 21 el *switch* de capa 3 se identifica de color negro, hace parte de la capa de núcleo.

[30] Dominio de Colisión: En Ethernet, el área de la red dentro del cual las tramas que han sufrido colisiones se propagan. Los repetidores y los hubs propagan las colisiones; los *switches* LAN, los puentes y los routers no lo hacen.

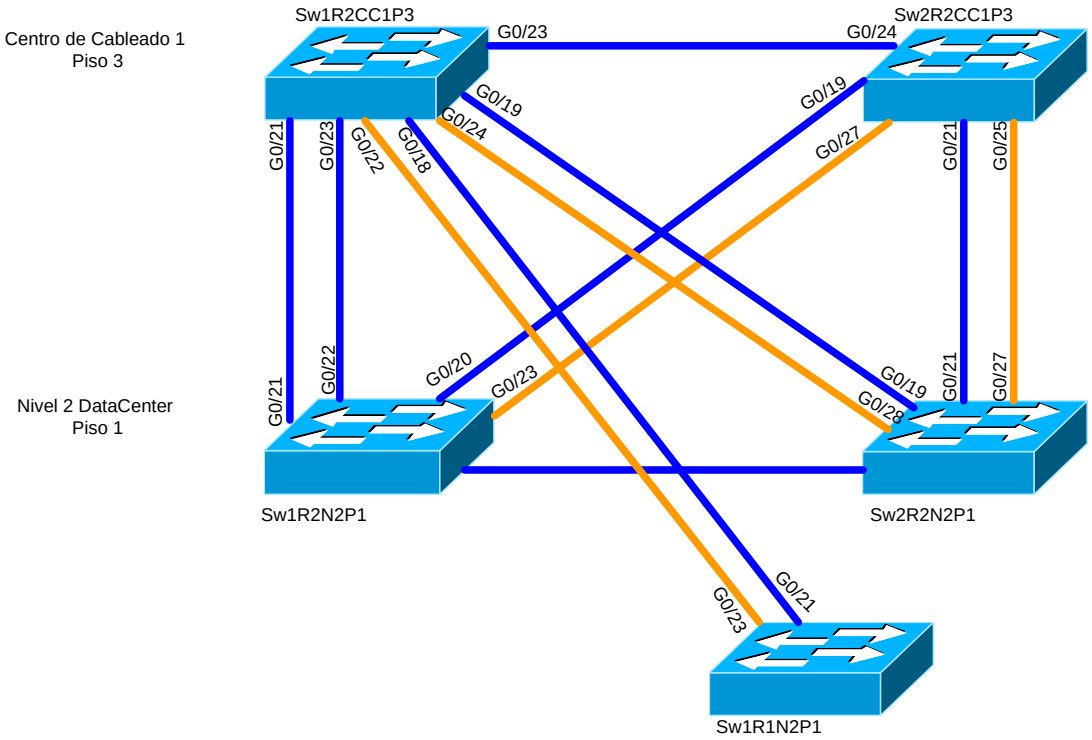
La capa de distribución en la figura 21 son todas las conexiones grises y verdes que hay de *switch* a *switch* y la función del *switch* de capa 3 de hacer el proceso de enrutamiento para la red.

4.2.7 Descripción de la Capa de núcleo

La capa núcleo de la reingeniería es el *backbone* de conmutación de alta velocidad. Esta capa del diseño de red no realiza ninguna manipulación de paquetes. La nueva red de SYC consta de una infraestructura central con rutas alternadas redundantes que ofrece estabilidad a la red en caso de que se produzca una única falla del dispositivo (ver figura 21). El re-diseño de la Red LAN se centra en la comunicación por medio de enlaces troncales (*trunks)*. Un enlace troncal es una conexión física y lógica entre dos *switches* a través de la cual viaja el tráfico de la red principal. Los *switches* CISCO de capa 2 y 3, entre sus características, tienen la capacidad de crear los enlaces *trunks* usados en el proyecto. El diseño del *backbone* del proyecto de reingeniería se aprecia en la figura 22, donde cada uno de los 5 *switches* que conforman el *backbone* tiene rutas redundantes y utiliza enlaces troncales de fibra (líneas naranjas) y cable de cobre UTP categoría 6 (líneas azules). Cada línea de enlace tiene de velocidad de 1 GigaE, se unen los enlaces que tienen dos líneas para el que el puerto *trunk* quede de 2 GigaE usando los *Port-Channels* que es una configuración que se puede hacer con los *switches* CISCO el cual se unen los enlaces *trunks* para así aumentar la velocidad del enlaces y tener más redundancia.

La figura 22 es la descripción detallada de cómo está diseñado el *backbone* del proyecto, los 5 *switches* son los mismos de la figura 21 que están en distinto color, el Sw2R2CC1P3 que quiere decir *switch* 2 rack 2 centro de cableado 1 piso 3 es *switch* de capa 3 identificado de color negro en la figura 21. La nomenclatura usada para nombrar los *switches* que conforman la red empresarial es explicada en la sección 4.3.2 Diseño e implementación de la capa 2.

Figura 22. Diseño de Backbone



AUTOR

4.3 SOLUCION E IMPLEMENTACION DEL PROYECTO

De acuerdo a los requisitos y características planteadas, la solución se basa en las piezas más importantes del diseño de una topología LAN, donde se encuentran las tres primeras capas del modelo OSI:

- El diseño e implementación de la capa 1 conocida como la capa física incluye el tipo de cableado a utilizar y la estructura global del cableado.
- El diseño e implementación de la capa 2 conocida como la capa de enlace presenta el *switch* LAN como el dispositivo usado la implementación del proyecto.
- El diseño e implementación de la capa 3 conocida como la capa de red utiliza un *switch* de capa 3 para crear segmentos LAN únicos, permitiendo la comunicación entre segmentos basando en el direccionamiento IP.

4.3.1 Diseño e implementación capa 1

Uno de los componentes más importantes a considerar en el diseño de red es el cableado físico. En la actualidad, la mayor parte del cableado LAN se basa en la tecnología Fast Ethernet o mejor aún en la tecnología Giga bit Ethernet.
"Giga bit Ethernet, también conocida como GigE, es una ampliación del estándar Ethernet que consigue una capacidad de transmisión de 1 giga bit por segundo, correspondientes a unos 1000 megabits por segundo de rendimiento contra unos 100 de Fast Ethernet".[31]
GigaE es la tecnología Ethernet que se ha actualizado de 100 Mbps a 1000 Mbps y tiene la capacidad de utilizar la funcionalidad full-duplex. Giga Ethernet utiliza la topología de bus lógica orientada a *broadcast* Ethernet estándar de 10BASE-T, y el método CSMA/CD para direcciones MAC.

Los temas de diseño en la Capa 1 incluyen el tipo de cableado que se debe utilizar, que normalmente se utiliza cable de cobre o fibra óptica y la estructura general del cableado. Para la tecnología Giga Ethernet, el tipo de cable utilizado es el par no blindado UTP de categoría 6 o el par blindado STP de categoría 6 y el cable de fibra óptica 100BaseFX.

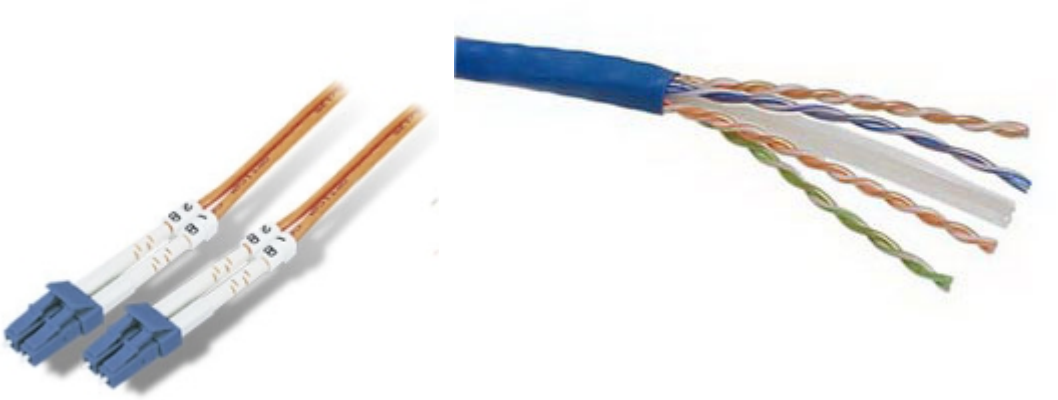
Los temas de Capa 1 provocan la mayoría de los problemas de red. Para la reingeniería se llevó a cabo una auditoría de cableado para planear los cambios significativos en la red. Esto ayudó a identificar las áreas que requerían actualizaciones y nuevo cableado.

El tipo de cableado a utilizar normalmente es el de cobre y fibra. Los medios de cableado utilizados por la auditoría fueron los UTP de Categoría 6 y el cable de fibra óptica multimodo (Ver figura 23). Se debe tener en cuenta que la red es diseñada para que dure de 7 a 10 años; por tanto, la calidad del cable debe ser una prioridad fundamental para la reingeniería.

---

[31] http://es.wikipedia.org/wiki/1000BASE-X

Figura 23. Medio de Cableado



Fuente.http://imagenes.solostocks.com/media/9/6/8/media_2420869.jpg
http://www.todoportatil.com.ve/venta/catalog/images/CLG04.jpg

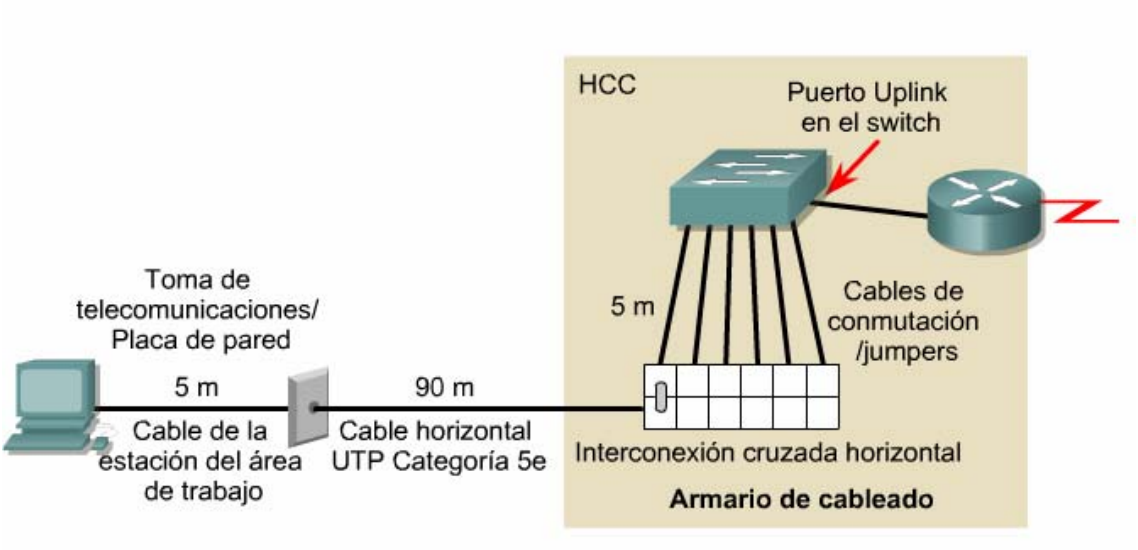
En todos los diseños de una red nueva o re-diseño de una red existente, normalmente se utiliza cable de fibra óptica para el *backbone* y cable de cobre UTP mínimo de categoría 5 para los tendidos horizontales de la red.

La empresa sigue el estándar TIA/EIA-568-A o B (ver ANEXO C.) que especifica que cada dispositivo conectado a la red debe estar conectado a una ubicación central a través de cableado horizontal. Esto se debe a que todos los hosts que necesitan acceso a la red deben estar dentro de un límite de distancia de 100 metros para el UTP Ethernet Categoría 6.

Los recintos de cableado de una topología estrella extendida se conocen como centros de cableado primario y secundario. Los centros de cableado primarios incluyen uno o más *patch pannels*[32] de conexión cruzada horizontal (*Horizontal cross connection,* HCC), como se muestre en la figura. 24

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

Figura 24. Centro de Cableado

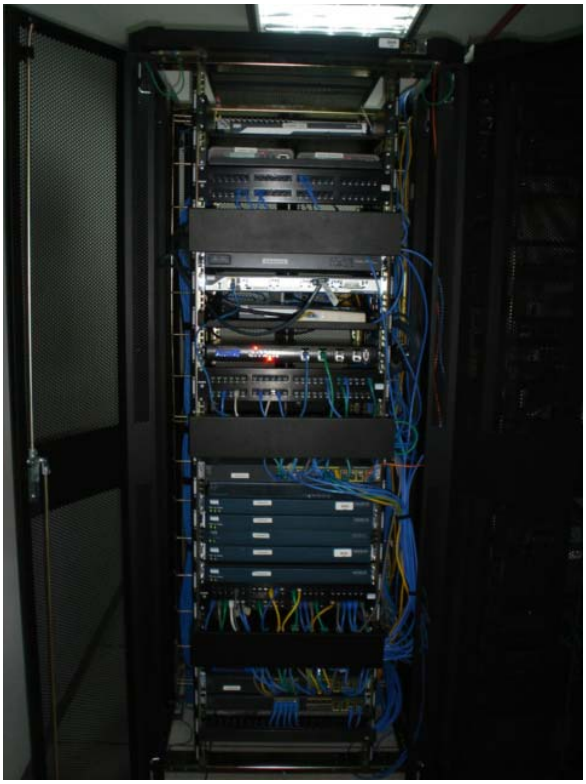


Fuente. Academia de Networking de Cisco Systems Guía del prime año CNNA 3 y 4 pág. 168. Marzo 2008

Cada puerto del *patch pannel* se utiliza para conectar el cableado horizontal de la capa 1 con los puertos del *switch* LAN de la capa 2, que a su vez comunica a una toma de comunicaciones que llega a una estación de área de trabajo como se muestra en la figura 24.

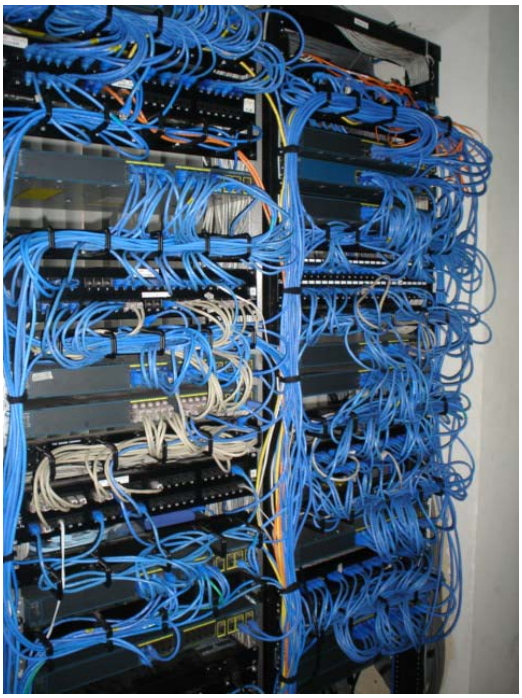
La empresa consta con varios centros de cableado primario y secundarios que implica la existencia de múltiples áreas de captación o conexión de puntos de la red. Existen dos centros de cableados primarios ubicados en el nivel 2 del DataCenter (figura 25) ubicado en el primer piso del Centro Empresarial Chicamocha y el Centro de Cableado 1 (figura 26) ubicado en la oficina principal de SYC en el tercer piso del centro empresarial. Los centros de cableados secundarios se encuentran alrededor de los diferentes departamentos que conforman la empresa.

Figura 25. Centro de Cableado Principal Data Center Nivel 2



Fuente. Autor

Figura 26. Centro de Cableado 1 Tercer piso SYC S.A

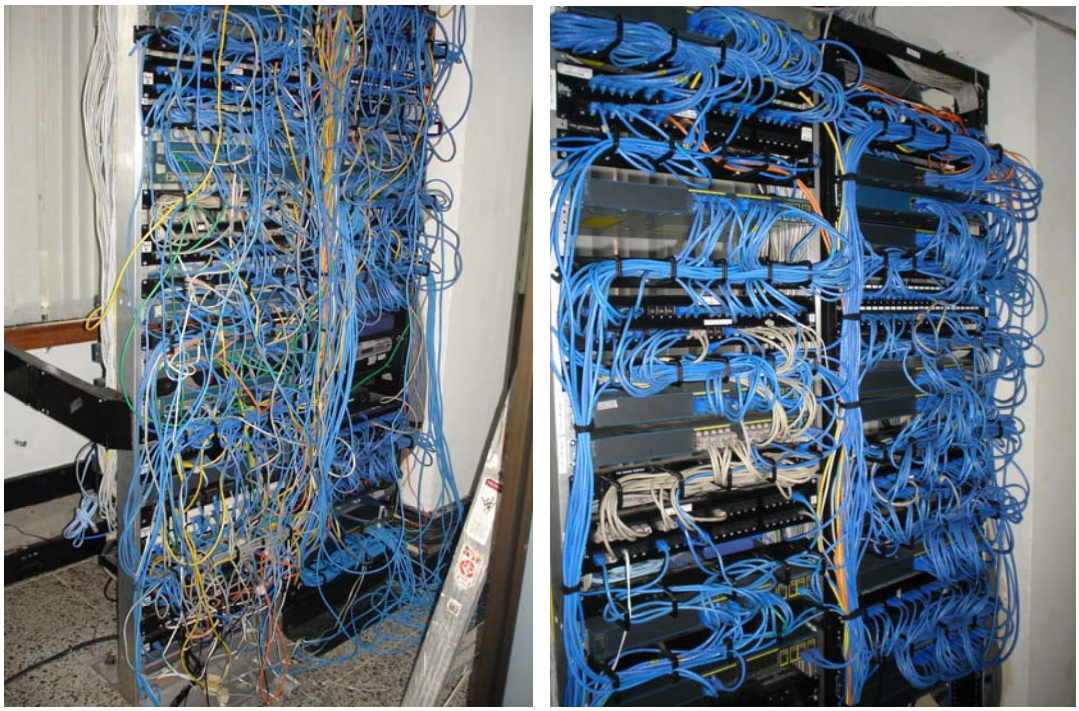


Fuente. Autor

Los estándares TIA/EIA -568-A que especifican que los dos centros de cableado primarios se deben conectar utilizando cableado vertical, también denominado cableado *backbone*. Para el *backbone*, normalmente se utiliza el cable de fibra óptica debido a que las longitudes del cable vertical son generalmente más largas que el límite de 100 metros del cable UTP Categoría 6. A su vez, la fibra óptica brinda más velocidad y menor tiempo de retardo. El proyecto de reingeniería consta de un *backbone* en fibra multimodo.

La figura 27 muestra un ejemplo del el antes y después de la auditoria nombrada para esta etapa de diseño.

Figura 27. Antes y después de la auditoria



Diciembre 2007 Marzo 2008

Fuente. Autor

4.3.2 Diseño e implementación capa 2

El propósito de los dispositivos de la Capa 2 en la red es conmutar tramas basadas en sus dirección es MAC destino, ofrecer detección de errores y reducir la congestión en la red. Aparte de la tarjeta de interfaz de red, que cualquier *host* de la red debe tener, el dispositivo más común de la capa 2 es el *switch* LAN. Como ya se había descrito, estos dispositivos determinan el tamaño de los dominios de colisión de la red.

El proyecto de reingeniería utiliza 30 *switches* de capa 2 ubicados en los diferentes recintos de cableado (ver tabla 3). La tabla 3, describe la cantidad de dispositivos usados, en que piso del centro empresarial está ubicado, el lugar de la empresa que se encuentra el dispositivo, la referencia del dispositivo, el nombre usado para identificarlo en la empresa, la dirección de red del dispositivo y si correspondiente MAC. La nomenclatura usada se identifica de esta manera: por ejemplo SW1CC1R1P3, esto significa *switch* 1 centro de cableado 1 rack 1 piso 3.

Por otro lado, los *switches* de la empresa tienen configurados las mismas VLAN'S utilizando el protocolo VTP. Donde cada proyecto o grupo de trabajo que conforma la empresa pertenece a una VLAN correspondiente, por lo que se pueden comunicar como si estuviesen en el mismo segmento físico de LAN. Esto facilita la administración de mudanzas, adiciones y cambios en los miembros de esos grupos o proyectos. En el esquema de direccionamiento del diseño de capa 3, encontramos la respectivas VLANs creadas para el proyecto de reingeniería.

La administración de los *switches*, una vez instalados y configurados en la infraestructura de red de la empresa, se hace por medio del sistema de gestión *CISCO NETWORK ASSISTANT, CNA (ver anexo D.)*.

Tabla 3. *Switches* capa 2 que conforma la infraestructura de red de SYC S.A.

# de Equipos	Piso	Lugar	Marca	Referencia	Nombre	Dirección	MAC
1	Piso 1 Datacenter	Nivel 1	Cisco	WS-C2960G-24TC-L	sw1d1n1p1	10.10.250.111	001d.46da.4e00
2	Piso 1 Datacenter	Nivel 1	Cisco	WS-C2960G-24TC-L	sw1d2n1p1	10.10.250.112	001c.f63c.c280
3	Piso 1 Datacenter	Nivel 1	Cisco	WS-C2960G-24TC-L	sw1d3n1p1	10.10.250.113	001d.46da.4000
4	Piso 1 Datacenter	Nivel 2	Cisco	WS-C2960G-24TC-L	sw1r1n2p1	10.10.250.121	001d.4609.6080
5	Piso 1 Datacenter	Nivel 2	Cisco	WS-C2960G-24TC-L	sw1r2n2p1	10.10.250.122	001d.46da.4d80
6	Piso 1 Datacenter	Nivel 2	Cisco	WS-C3560G-24TS	sw2r2n2p1	10.10.250.123	001d.e5c3.4500
7	Piso 1 Datacenter	Nivel 3	Cisco	WS-C2960G-24TC-L	sw1r4n3p1	10.10.250.134	001c.f9ef.b280
8	Piso 1 Datacenter	Nivel 3	Cisco	WS-C2960G-24TC-L	sw1r8n3p1	10.10.250.138	001d.46d9.5c00
9	Piso 1 Datacenter	Nivel 3	Cisco	WS-C2960G-24TC-L	sw1r6n3p1	10.10.250.136	001d.46da.4580
10	Piso 1 Datacenter	Nivel 3	Cisco	WS-C2960G-24TC-L	sw1r7n3p1	10.10.250.137	001b.0d99.8c80
11	Piso 1 Datacenter	Nivel 3	Cisco	WS-C2960G-24TC-L	sw1r5n3p1	10.10.250.135	001d.4609.4880
12	Piso 3	CC1	Cisco	WS-C2960G-24TC-L	sw1cc1r1p3	10.10.250.201	001d.46d9.ae80
13	Piso 3	CC1	Cisco	WS-C2960G-24TC-L	sw2cc1r1p3	10.10.250.202	001c.f940.b700
14	Piso 3	CC1	Cisco	WS-C2960G-24TC-L	sw3cc1r1p3	10.10.250.203	001c.f63c.a980
15	Piso 3	CC1	Cisco	WS-C2960G-24TC-L	sw4cc1r1p3	10.10.250.204	001c.f9ef.c280
16	Piso 3	CC1	Cisco	WS-C2960G-24TC-L	sw5cc1r1p3	10.10.250.205	001c.b1c9.8200
17	Piso 3	CC1	Cisco	WS-C2960G-24TC-L	sw3cc1r2p3	10.10.250.213	001c.b1ba.5580
18	Piso 3	CC1	Cisco	WS-C2960G-24TC-L	sw4cc1r2p3	10.10.250.214	001d.46da.1680
19	Piso 3	CC1	Cisco	WS-C2960G-24TC-L	sw5cc1r2p3	10.10.250.215	001c.f9ef.b700
20	Piso 3	CC1	Cisco	WS-C2960G-24TC-L	sw6cc1r2p3	10.10.250.216	001d.46da.b900
21	Piso 3	CC1	Cisco	WS-C2960G-24TC-L	sw7cc1r2p3	10.10.250.217	001c.f63d.8400
22	Piso 3	CC2	Cisco	WS-C2960G-24TC-L	sw1cc2p3	10.10.250.231	001c.f63d.1e00
23	Piso 3	CC2	Cisco	WS-C2960G-24TC-L	sw2cc2p3	10.10.250.232	001c.f63c.1880
24	Piso 3	CC2	Cisco	WS-C2960G-24TC-L	sw3cc2p3	10.10.250.233	00ib.0d99.a480
25	Piso 3	CC2	Cisco	WS-C2960G-24TC-L	sw4cc2p3	10.10.250.234	001d.46d9.ab80
26	Piso 2	ING	Cisco	WS-C2960G-24TC-L	s1minip2	10.10.250.161	001d.46da.aa00
27	Piso 2	ING	Cisco	WS-C2960G-24TC-L	s2minip2	10.10.250.162	001c.f63c.ce00
28	Piso 2	ING	Cisco	WS-C2960G-24TC-L	s3minip2	10.10.250.163	001d.46da.ce80

29	Piso 2	Editorial	Cisco	WS-C2960G-24TC-L	s1cc1p2	10.10.250.151	001d.46d9.5c80
30	Piso 2	Editorial	Cisco	WS-C2960G-24TC-L	S2cc1p2	10.10.250.152	001d.e688.f480

Fuente. Autor

Los *switches* de la topología física de SYC S.A (ver figura 28), se pueden identificar con ayuda de la tabla 3. Esta figura muestra los nombres de los *switches* y todas la conexiones *switch* a *switch* por medio de enlaces *trunks* explicados en la sección *2. Marco teórico 2.8.* La mayoría de los *switches* tienen enlaces redundantes, esto quiere decir que tiene más de un puerto *trunk* en un *switch*. Cada enlace utiliza solo cierto grupo de VLANs. Es decir pasan unas VLANs por un enlace y las otras por el otro enlace, esto se identifica en la figura por el color gris del túnel de enlace, ya que cuando es de color verde quiere decir que todas las VLANs pasan por ese enlace.

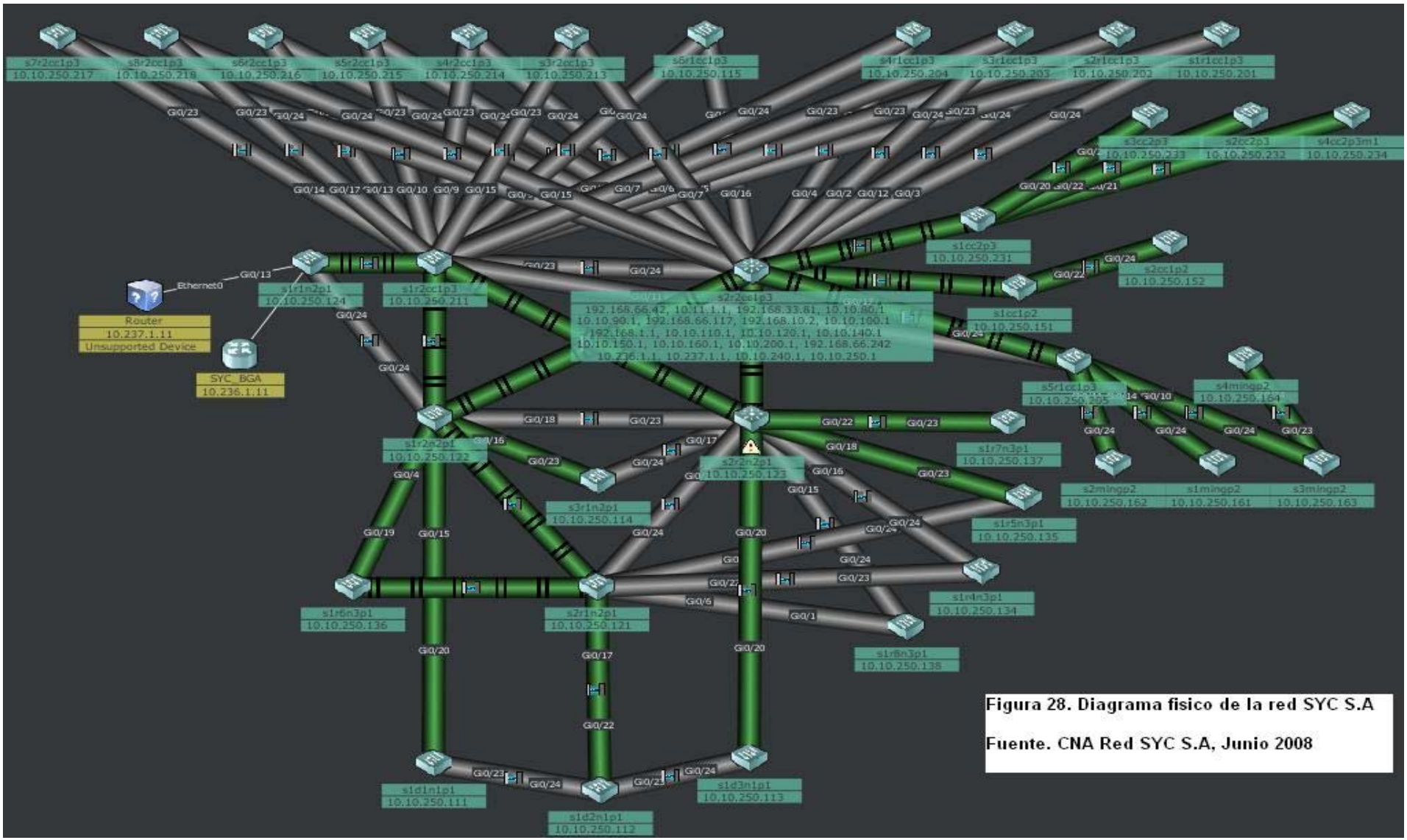


Figura 28. Diagrama fisico de la red SYC S.A

Fuente. CNA Red SYC S.A, Junio 2008

4.3.3 Diseño e implementación capa 3

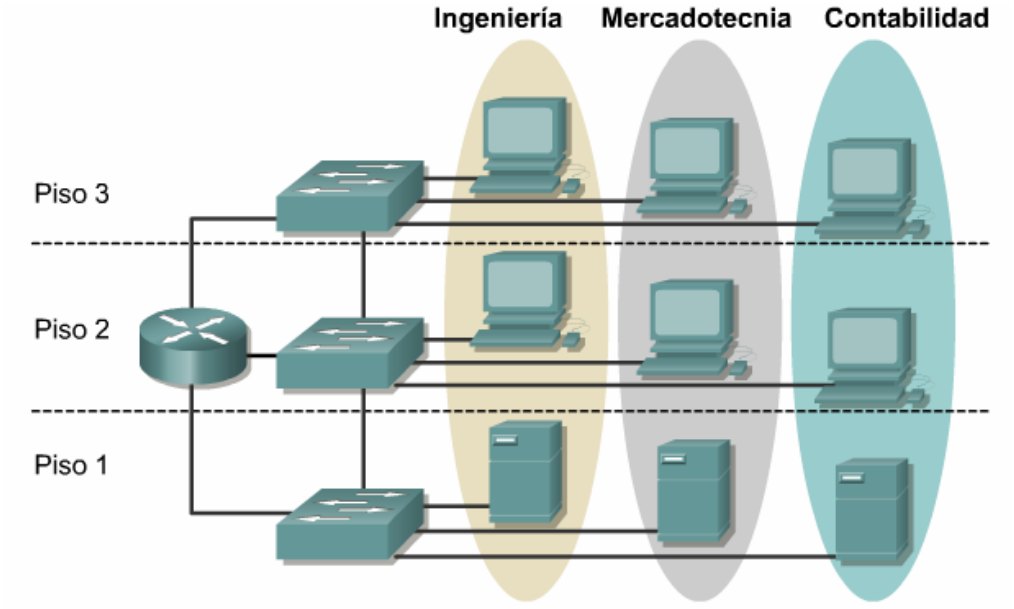
"Los dispositivos de la Capa 3 se utilizan para crear segmentos LAN únicos, también permiten la comunicación entre los segmentos basados en las direcciones de Capa 3, como por ejemplo direcciones IP. La implementación de los dispositivos de Capa 3 permite la segmentación de la LAN en redes lógicas y físicas exclusivas. También permiten la conectividad a las WAN como, por ejemplo, Internet."[33]

En todo diseño de red, el enrutamiento de Capa 3 determina el flujo de tráfico entre los segmentos de red física exclusivos basados en direcciones de Capa 3. En el presente proyecto, un *switch* de capa 3 trabaja como router enviando paquetes de datos basados en direcciones destino. El *switch* Catalyst 3560G de CISCO es de capa 3 y tiene las características de un router, de manera que no envía *broadcast* basados en LAN, tales como las peticiones ARP. Por lo tanto, la interfaz del *switch* de capa 3 se considera como el punto de entrada y salida de un *dominio de broadcast* y evita que los *broadcast* lleguen hasta los otros segmentos LAN.

Las VLANs utilizadas en el proyecto "pueden limitar el tráfico de difusión al interior de un VLAN y crear dominios de difusión más pequeños." En este proyecto se utilizan las VLAN para proporcionar seguridad, teniendo así una VLAN por cada grupo de trabajo o proyecto. Como anteriormente se explicó esto limita el tamaño de los dominios de difusión y se utiliza un router o un *switch* de capa 3 para determinar si una VLAN puede hablar con otra VLAN, dando así un esquema de seguridad basado en la asignación VLAN como se puede notar en la figura 29.

[33] *Academia de Networking de Cisco Systems Guía del primer a;o CCNA 3 y 4 pág. 177-178*

Figura 29. Ejemplo de asignación de VLANs



Fuente. Academia de Networking de Cisco Systems Guía del prime año CNNA 3 y 4 pág. 179. Marzo 2008

Con esto se garantiza fluidez de tráfico e independencia entre los diferentes grupos organizativos de la empresa. Los dispositivos de capa 3 ofrecen una mayor escalabilidad, dividiendo las redes y las subredes, añadiendo así una estructura de direcciones IP. La empresa, que presentaba problemas de escalabilidad, dio solución a esto dividiendo la red en subredes, utilizando un esquema simple de direcciones.

Las direcciones IP que no están asignadas se denominan direcciones privadas. "Las direcciones privadas pueden ser utilizadas por los hosts que usan traducción de dirección de red (*Network* address translation, *NAT*) para conectarse a una red pública o por los hosts que no se conectan a Internet. En una misma red no puede existir dos direcciones iguales, pero tales direcciones sí se pueden repetir en dos redes privadas que no tengan conexión entre sí o que se sea a través de NAT."[34]

[34] http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP

Una red privada es una red que usa el espacio de direcciones IP especificadas en el documento RFC 1918 (ver anexo E.). Las organizaciones utilizan este espacio de direcciones cuando requieran que ellas deban comunicarse dentro de la red interna.

Como ya antes se mencionó, el dispositivo capa 3 utilizado para la comunicación entre segmentos basándose en el direccionamiento IP en el proyecto de reingeniería de la infraestructura de red LAN de SYC S.A es el *switch* CISCO 3560G de capa 3 donde se describe en la tabla 5.

Tabla 4. *Switches* de capa 3

# de Equipos	Piso	Lugar	Marca	Referencia	Nombre	Dirección	MAC
1	Piso 1 Datacenter	Nivel 2	Cisco	WS-C3560G-24TS	sw2r2n2p1	10.10.250.123	001c.f9ef.c380
2	Piso 3	CC1	Cisco	WS-C3560G-24TS	sw2cc1r2p3	10.10.250.1	001d.4644.2b00

Fuente. Autor

Para la reingeniería se tomó un rango de direcciones clase A que está comprendido entre 10.0.0.0 y 10.255.255.255, que es un rango de direcciones privadas según el documento RFC 1918. Así, se aplicó una división de subredes conocido como *subnetting*, donde, utilizando cada sub red para una VLAN diferente que maneja un grupo de trabajo o proyecto de la empresa. La división realizada en las direcciones se observa en la tabla 6.

Tabla 5. Esquema de direccionamiento para proyectos SYC S.A.

CLASE A: 10.10.0.0 255.255.255.0

Host hábiles: 253 por VLAN

Numero de VLAN	Dirección IP	Nombre de VLAN
Vlan1	unassigned	1 default
Vlan2	192.168.1.1	2 SubRed_1
Vlan3	172.16.1.1	3 SubRed_Dmz
Vlan4	192.168.10.2	4 SubRed_10
Vlan7		7 SubRed_FlyconInternet
Vlan8	10.236.1.1	8 SubRed_FlyconIss
Vlan9		9 SubRed_EtbInternet
Vlan10	10.237.1.1	10 SubRed_EtbTorreC
Vlan11		11 SubRed_EtbInternet1
Vlan70	10.10.70.1	70 SubRed_Iuva1
Vlan80	10.10.80.1	80 Pry_Iss
Vlan90	10.10.90.1	90 Captura
Vlan100	10.10.100.1	100 Ingenieria
Vlan110	10.10.110.1	110 Administrativa
Vlan120	10.10.120.1	120 Contabilidad
Vlan130	10.10.130.1	130 Estampillas
Vlan140	10.10.140.1	140 Red_Iuva_Registro
Vlan150	10.10.150.1	150 SubRed_Syc_Editorial
Vlan160	10.10.160.1	160 SubRed_Corporativa
Vlan200	10.10.200.1	200 IT-Services
Vlan250	10.10.250.1	250 Management

Fuente. Autor

En la tabla 4, podemos observar que los *switches* CISCO por defecto tienen la VLAN 1, pero para la re ingeniería no se tiene en cuenta, solo se ignora, esto se debe a que por defecto los *switches* en su configuración inicial los puertos pertenecen a esta VLAN y es la única VLAN que no se puede borrar ya que el sistema operativo no deja.

Es importante aclarar que la VLAN 2 (SubRed_1) y la VLAN 4 (SubRed_10) fueron creadas para el proceso de migración de la re ingeniería. La empresa, como anteriormente fue explicado, trabajaba con estas dos sub redes para su red empresarial. Estas 2 VLAN tienden a desaparecer.

Por su parte, la VLAN 3 (SubRed_Dmz) como su nombre lo indica corresponde al segmento de la DMZ que tiene los servidores de la empresa.
Las VLAN 7 (SubRed_FlyconInternet), Vlan 8 (SubRed_FlyconIss), Vlan 9 (SubRed_EtbInternet), Vlan 10 (SubRed_EtbTorreC) y la Vlan 11 (SubRed_EtbInternet1) corresponden a los enlaces dedicados y las salidas de internet de la empresa.
Por último la Vlan 250 corresponde a todos los dispositivos de red (*switches*). El resto de VLAN correspondes a los proyectos y grupos de trabajo que conforman la empresa. Fueron creadas para separar el tráfico dentro de la red.

El *switch* de capa 3 con referencia 3560G, limita el tamaño de los *dominios de broadcast* y determina por medio de rutas estáticas si puede haber comunicación de una VLAN con otra. Las siguientes líneas pertenecen a la configuración de rutas que tiene el *switch* 3560G de CISCO perteneciente a la empresa Sistemas Y Computadores S.A. Según los códigos del comando mostrado, la “C” define los segmentos de dirección IP que están directamente conectado al *switch* y la “S” define las rutas estáticas creadas en el *switch* de capa 3.

Show ip route:

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.10.0/24 is directly connected, Vlan4
172.16.0.0/24 is subnetted, 1 subnets
S 172.16.2.0 [1/0] via 192.168.10.81

192.168.11.0/32 is subnetted, 1 subnets
S 192.168.11.26 [1/0] via 192.168.10.1
200.21.252.0/32 is subnetted, 1 subnets
S 200.21.252.229 [1/0] via 10.10.80.3
192.168.66.0/24 is variably subnetted, 3 subnets, 2 masks
C 192.168.66.32/28 is directly connected, Vlan301
C 192.168.66.112/29 is directly connected, Vlan307
C 192.168.66.240/29 is directly connected, Vlan305
10.0.0.0/8 is variably subnetted, 19 subnets, 4 masks
S 10.1.0.0/16 [1/0] via 192.168.10.1
S 10.1.5.1/32 [1/0] via 192.168.10.1
S 10.20.0.0/16 [1/0] via 10.237.1.11
C 10.10.80.0/24 is directly connected, Vlan80
C 10.10.90.0/24 is directly connected, Vlan90
C 10.10.100.0/24 is directly connected, Vlan100
C 10.10.110.0/24 is directly connected, Vlan110
C 10.10.120.0/24 is directly connected, Vlan120
C 10.10.140.0/24 is directly connected, Vlan140
S 10.10.141.0/24 [1/0] via 192.168.10.1
S 10.10.145.0/29 [1/0] via 192.168.10.1
C 10.10.150.0/24 is directly connected, Vlan150
C 10.10.160.0/24 is directly connected, Vlan160
C 10.10.200.0/24 is directly connected, Vlan200
C 10.237.1.0/24 is directly connected, Vlan10
C 10.236.1.0/24 is directly connected, Vlan8
C 10.10.240.0/24 is directly connected, Vlan240
C 10.10.250.0/24 is directly connected, Vlan250
S 10.240.1.0/24 [1/0] via 10.237.1.11
C 192.168.1.0/24 is directly connected, Vlan2
S 192.168.2.0/24 [1/0] via 192.168.10.1
S 192.168.3.0/24 [1/0] via 192.168.10.1
C 192.168.33.0/24 is directly connected, Vlan6

Los enlaces de telecomunicaciones utilizados en la empresa permiten el acceso desde y hacia Internet y las conexiones punto a punto, llamadas enlaces dedicados, que son requeridos para proyectos específicos. En la tabla 7 y 8 se presenta la descripción de los routers usados por los proveedores de servicio que tienen las siguientes características básicas:

- Empresa de Teléfonos de Bogotá E.T.B
    - Enlace dedicado Syc Bucaramanga – Syc Bogota (2048 Mbps)
    - Enlace dedicado Syc Bucaramanga – Syc Cali (2048 Mbps)
    - Enlace Internet (2048 Mbps)
- Internexa S.A – Flycom
    - Enlace dedicado Syc Bucaramanga – ISS Bogotá (1024 Mbps)
    - Enlace Internet (2048 Mbps)

Tabla 6. Routers para enlaces ETB

# de Equipos	Piso	Lugar	Marca	Referencia	Nombre	Dirección de int ETH	MAC de int ETH	Enlace
1	Piso 1 Datacenter	Nivel 2	Cisco	Router 2509	Router	10.237.1.11	0010.7b3b.9a1f	SYC Bogota
2	Piso 1 Datacenter	Nivel 2	Cisco	Router 2801	SISTE_COMPUTAD_BUC_PPAL	192.168.3.17	0019.56CA.5F42	SYC Cali
3	Piso 1 Datacenter	Nivel 2	Cisco	Router 1841	Siste_compu_Buc_In	eth 0/0: 190.24.11.193	001b.d5ee.d65a	Internet
						eth 0/1: 200.75.44.97	001b.d5ee.d65b	

Fuente. Autor

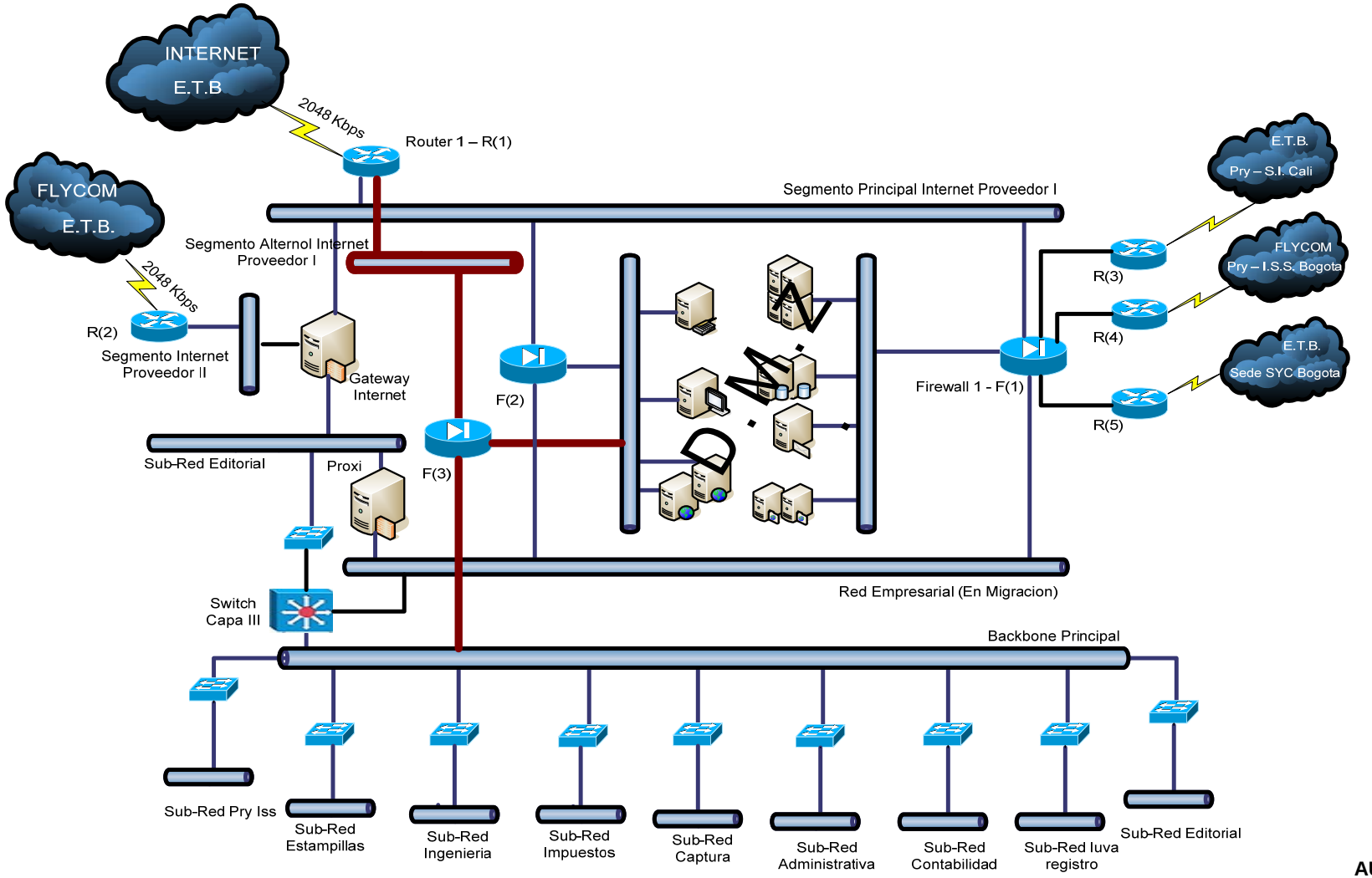
Tabla 7. Routers para enlaces Flycom

# de Equipos	Piso	Lugar	Marca	Referencia	Nombre	Dirección de int ETH	MAC de int ETH	Enlace
1	Piso 1 Datacenter	Nivel 2	Cisco	Router 1841	SYC_BGA	10.236.1.11 190.90.32.209	0011.216c.c683	Internet; ISS. Bogotá

Fuente. Autor

Por último la solución planteada para el proyecto de reingeniería de la infraestructura de red LAN de SYC S.A se resume en la topología lógica que se describe en la figura 30. La topología lógica del proyecto, identifica las subredes creadas para los distintos proyectos organizativos de la empresa y utilizando el *switch* de capa 3 para enrutar las VLANs y tener comunicación en toda la red empresarial. La figura muestra el uso de firewalls cuya función es brindar seguridad en la entrada de a la DMZ. La seguridad en este segmento tiene que ser considerada, ya que es la red de servidores de la empresa SYC S.A. También la topología describe los enlaces de internet y canales dedicados que se tiene con los diferentes proveedores y como entran a la red LAN empresarial. Se nota un gran cambio con respecto a la topología lógica inicial mostrada en la figura 18. Los problemas presentados se ven corregidos en el diseño implementado, alcanzando así los requisitos de la empresa planteados alrededor de este proyecto.

Figura 30. Topología lógica de SYC S.A



AUTOR

5 METODO DE CONFIGURACION DE LOS DISPOSITIVOS DE RED

Una vez se hizo el levantamiento de información inicial de infraestructura se empezó a trabajar con los equipos 2960G de la serie 2900 de CISCO y el 3560G de la serie 3500 de CISCO.

Inicialmente antes de implementar el proyecto se plantearon laboratorios para verificar que las VLAN podían ser definidas en los *switches* capa 2 y por otro lado que estas VLAN pudieran verse con otras a través del *switch* de capa 3 por medio de las funciones de *routing*. Las pruebas realizadas se concentraron básicamente en comprobar la conectividad de las VLAN de capa 2, ya que por default todos los puertos del *switch* pertenecen a la VLAN 1 y por otro lado establecer que efectivamente se pudieran ver las distintas VLAN a través del *switch* de capa 3. A su vez se hicieron pruebas de comportamiento de los puertos cuando se definen como *trunks* o *port-channel* para los distintos *switches*, tratando de establecer si operaban como dice la teoría.

Según la teoría de CISCO, dice que los puertos que se definen como *port-channel*, presentan una contingencia en donde si llegara el caso de caerse unos de los enlaces, no se percibe la caída y el tráfico de datos sigue trabajando sin notar ningún cambio, aparte la unión de enlaces aumenta la velocidad sumando los puertos *trunks* convirtiendo en un solo enlace. Por otro lado cuando se tiene un puerto modo *trunk* y se cae, de manera inmediata el tráfico se asume por otro puerto *trunk* si llega a existir, pero cuando es *port-channel* la red ni siquiera percibe la caída y todo sigue funcionando de manera normal. Y así, se identifica la ventaja de trabajar y configura los *port-channel* en la red que son de gran uso para el *backbone* del proyecto de reingeniería.

Las siguientes prácticas de laboratorios se llevaron a cabo en el DataCenter de la empresa Sistemas y Computadores. En cada práctica se tiene en cuenta la tabla 8 que describe los modos de comando de configuración de un *switch*

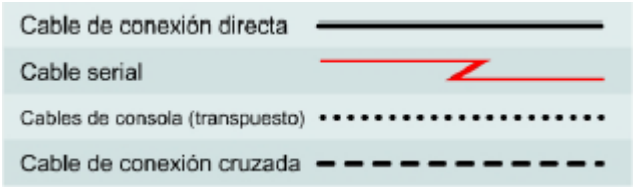
CISCO, y la figura 31 que muestra la grafica de líneas de conexión para el uso de las prácticas de laboratorio.

Tabla 8. Modos de comando de *switch* CISCO

Modos de comando del switch			
Modo de comando	**Método de acceso**	**Indicador del switch que aparece**	**Método de salida**
EXEC usuario	Iniciar una sesión	`Switch>`	Use el comando **`logout`**.
EXEC Privilegiado	En el modo EXEC usuario, introduzca el comando **`enable`**.	`Switch#`	Para salir al modo EXEC usuario, use el comando **`disable`**, **`exit`**, o **`logout`**.
Configuración global	Desde el modo EXEC privilegiado, introduzca el comando **`configure terminal`**.	`Switch(config)#`	Para salir al modo EXEC privilegiado, use el comando **`exit`** o **`end`**, o presione Ctrl-z.
Configuración de la interfaz	En el modo de configuración global, introduzca el comando **`interface type number`**, como, por ejemplo, **`interface serial 0`**.	`Switch(config-if)#`	Para salir al modo de configuración global, use el comando **`exit`**.

Fuente. CCNA 3: Principio básicos de conmutación y enrutamiento intermedio v3.1 Manual de laboratorio para el estudiante

Figura 31. Grafica de línea de conexión para prácticas de laboratorio.

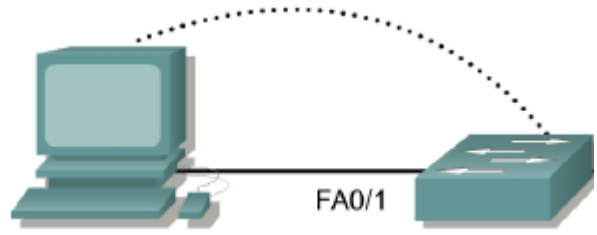


Fuente. CCNA 3: Principio básicos de conmutación y enrutamiento intermedio v3.1 Manual de laboratorio para el estudiante

5.1 Practica 1. Verificación de la configuración por defecto del *switch*

Figura 32. Grafica de guía para las prácticas 1 y 2.

.

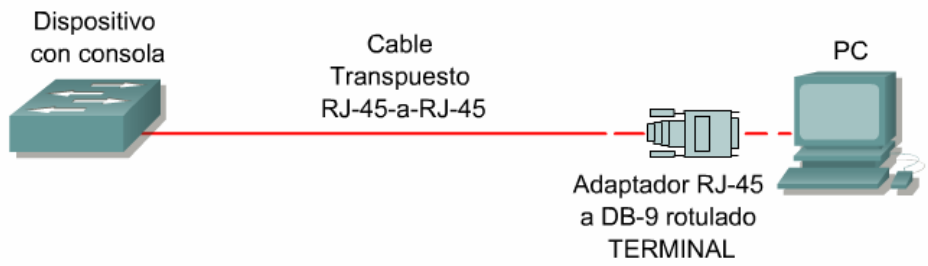


Fuente. CCNA 3: Principio básicos de conmutación y enrutamiento intermedio v3.1 Manual de laboratorio para el estudiante

Paso 1 conexión al puerto de consola y configuración del puerto

Para poder configurar o verificar el estado de un *switch*, se conecta una computadora al *switch* para establecer una sesión de comunicación. Se Utiliza un cable transpuesto o *rollover* para conectar el puerto de consola de la parte trasera del *switch* a un puerto COM en la parte trasera de la computadora, como dice la figura 33.

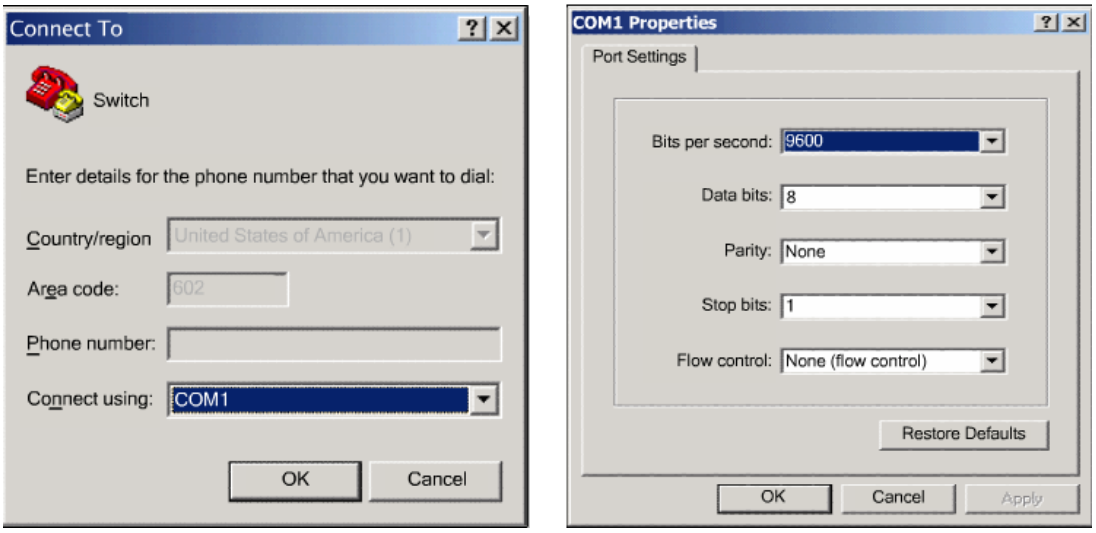
Figura 33. Conexión del *switch* al PC



Fuente. CCNA 3: Principio básicos de conmutación y enrutamiento intermedio v3.1 Manual de laboratorio para el estudiante

Se Inicia el *HyperTerminal*[35] en la computadora. Primero debe otorgarse un nombre a la conexión al configurar por primera vez la comunicación de *HyperTerminal* con el *switch*. Seleccione el puerto COM al cual el *switch* está conectado desde el menú desplegable y haga clic en el botón OK (Figura34). Aparece otra ventana de diálogo. Establezca los parámetros tal como aparecen en la Figura 34 y haga clic en el botón OK.

Figura 34. Parámetros de configuración del puerto



Fuente. CCNA 3: Principio básicos de conmutación y enrutamiento intermedio v3.1 Manual de laboratorio para el estudiante

Una vez que el *switch* ha arrancado, aparecen indicadores de diálogo de Configuración del Sistema.

[35] HyperTerminal es una aplicación que puede utilizar con el fin de conectar su ordenador a otros sistemas remotos. Estos sistemas incluyen otros ordenadores, los sistemas de tablón de anuncios, servidores, sitios Telnet, y los servicios en línea. Sin embargo, usted necesita un módem, una conexión Ethernet, o un cable null módem antes de que pueda utilizar HyperTerminal.

Paso 2 Entrar al modo privilegiado

El modo privilegiado da acceso a todos los comandos del *switch*. Muchos de los comandos privilegiados configuran los parámetros de operación. Por lo tanto, el acceso privilegiado debe estar protegido mediante contraseñas para evitar el uso no autorizado. El conjunto de comandos privilegiados incluye aquellos comandos del modo EXEC usuario, así como también el comando configure a través del cual se obtiene acceso a los modos de comando restantes.

Switch>**enable**
Switch#

Paso 3 Examinar el archivo de configuración activo

Examine el archivo de configuración activa actual.

Switch#**show running-config**

En la configuración se identifica cuantos puertos Ethernet, Fast Ethernet o Giga Ethernet tiene el *switch* y el intervalo de valores q se muestran para las líneas VTY. Para *switch* CISCO 2960G tiene 24 puerto Giga Ethernet y los valores VTY son de 0 al 15

Paso 4 Mostrar información acerca del IOS

Examine la siguiente información acerca de la versión generada por el *switch*.

Switch#**show version**

Paso 5 Examinar las interfaces Fast Ethernet

Examine las propiedades por defecto de las interfaces Giga Ethernet.

#**show interface**

5.2 Practica 2. Configuración básica de un *switch*

Paso 1 Asignar un nombre al *switch*

Se escribe *enable* y luego el modo de configuración. El modo de configuración permite la gestión del *switch*. Se cambio el nombre de defecto del *switch* por Sw1n1p1, este es el nombre con el que se hará referencia a este *switch*:

Switch#**configure terminal**
Introduzca los comandos de configuración, uno por cada línea. Finalice presionando **Ctrl-Z**.
Switch(config)#**hostname Sw1n1p1**
Sw1n1p1(config)#**exit**

Paso 2 Configurar las contraseñas de acceso

Entrar al modo de configuración de línea para la consola. Establecer SYC como contraseña en esta línea para iniciar una sesión. Configure las líneas VTY[36] 0 a 15 con la contraseña SYC:

Sw1n1p1#**configure terminal**
Introduzca los comandos de configuración, uno por cada línea. Finalice presionando **Ctrl-Z**.
Sw1n1p1(config)#**line con 0**
Sw1n1p1(config-line)#**password SYC**
Sw1n1p1(config-line)#**login**
Sw1n1p1(config-line)#**line vty 0 15**
Sw1n1p1(config-line)#**password SYC**
Sw1n1p1(config-line)#**login**
Sw1n1p1(config-line)#**exit**

Paso 3 Configurar las contraseñas de los modos de comando

Establecer *enable password* en SYC y enable secret password en class:

Sw1n1p1(config)#**enable password cisco**
Sw1n1p1(config)#**enable secret class**

[36] Comando que se usa para establecer una protección mediante contraseña para las sesiones Telnet entrantes en el caso del *switch* son del 0 a 15.

Paso 4 Configurar la capa 3 para obtener acceso al *switch* por telnet.

Establecer la dirección IP del *switch* en 10.10.250.2 con una máscara de subred 255.255.255.0

Sw1n1p1(config)#**interface VLAN 1**
Sw1n1p1(config-if)#**ip address 10.10.250.2 255.255.255.0**
Sw1n1p1(config-if)#**exit**

Establecer el *gateway* por defecto para el *switch* y la VLAN de administración por defecto en 10.10.250.1:

Sw1n1p1(config)#**ip default-gateway 10.10.250.1**
Sw1n1p1(config)#**exit**

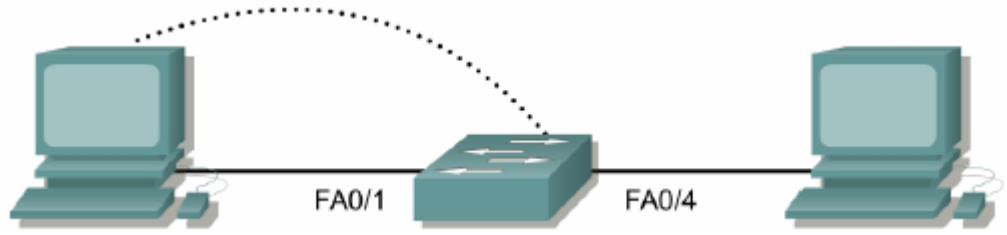
Paso 8 Verificar los parámetros de administración de las LAN

Verificar que los valores de la interfaz de la VLAN 1:

Sw1n1p1#**show interface VLAN 1**
Habilite la interfaz virtual por medio del comando **no shutdown**
Sw1n1p1(config)#**interface VLAN 1**
Sw1n1p1(config-if)#**no shutdown**
Sw1n1p1(config-if)#**exit**

5.3 Practica 3. Administración de la tabla de direcciones MAC

Figura 35. Grafica de guía para la prácticas 3.



Fuente. CCNA 3: Principio básicos de conmutación y enrutamiento intermedio v3.1 Manual de laboratorio para el estudiante

Tabla 9. Tabla de configuración de la practica 3.

Designación del *switch*	Nombre del *switch*	Contraseña enable secret	Contraseñas enable, de VTY y de Consola	Dirección IP de VLAN 1	IP del Gateway por defecto	Mascara de subred
Switch 1	Sw1n1p1	class	SYC	10.10.250.2	10.10.250.1	255.255.255.0

AUTOR

Paso 1 Configurar los hosts conectados al *switch*

Configurar los hosts para que utilicen la misma subred IP para la dirección, máscara y *gateway* por defecto que el *switch*.

Paso 2 Verificar la conectividad

Para verificar que los hosts y el *switch* estén configurados correctamente, hacer un ping a la dirección IP del *switch* desde los hosts.

Ping 10.10.250.2 es exitoso

Paso 3 Determinar las direcciones MAC que el *switch* ha aprendido

Para determinar las direcciones MAC que el *switch* ha aprendido, usar el comando show macaddress-table en el indicador del modo EXEC privilegiado:

```
Sw1n1p1#show mac-address-table
```

Paso 4 Borrar la tabla de direcciones MAC

Para eliminar las direcciones MAC existentes, se usa el comando clear mac-address-table en el indicador del modo EXEC privilegiado:

```
Sw1n1p1#clear mac-address-table dynamic
```

Paso 5 Configurar una dirección MAC estática

Configurar una dirección MAC estática en la interfaz Giga Ethernet 0/4:
Nota: la dirección que se registra a continuación, la dirección MAC 00e0.2917.1884 se usa en la sentencia para ejemplo. Se Usa la dirección del PC conectado al puerto Giga Ethernet 0/4 del *switch*.

```
Sw1n1p1(config)#mac-address-table static 00e0.2917.1884 interface
gigabiteethernet 0/4 vlan 1
```

Paso 6 Eliminar la entrada MAC estática

Es posible que sea necesario eliminar la entrada static mac-address-table. Para hacer esto, entre al modo de configuración y deshaga el comando colocando “no” delante de toda la cadena de comandos anterior:
Nota: La dirección MAC 00e0.2917.1884 se usa solamente en la sentencia del ejemplo. Se usa la utilizada para la practica en el paso 4.

```
Sw1n1p1(config)#no mac-address-table static 00e0.2917.1884 interface
gigabiteethernet 0/4 vlan 1
```

Paso 7 Anotar las opciones de seguridad de puerto

Determine cuáles son las opciones para configurar la seguridad de puerto en la interfaz Gigabiteethernet 0/4

```
Sw1n1p1(config-if)#switchport port-security ?
aging Port-security aging commands
mac-address Secure mac address
maximum Max secure addrs
violation Security Violation Mode
<cr>
```

Para permitir que el puerto de *switch* Gigabiteethernet 0/4 acepte sólo un dispositivo, introduzca port security como se indica a continuación:

```
Sw1n1p1(config-if)#switchport mode access
Sw1n1p1(config-if)#switchport port-security
Sw1n1p1(config-if)#switchport port-security mac-address sticky
```

Paso 8 Verificar los resultados

Introducir el siguiente comando para verificar las entradas de la tabla mac–address table.

```
Sw1n1p1#show mac-address-table
```

Mostrar los valores de seguridad de puerto con el siguiente comando.

```
Sw1n1p1#show port-security
```

Paso 9 Limitar la cantidad de hosts por puerto

En la interfaz Gigabiteethernet 0/4, configurar en 1 el número máximo de MAC para la seguridad de puerto:

```
Sw1n1p1(config-if)#switchport port-security maximum 1
```

Paso 10 Configurar el puerto para que se desconecte si se produce una violación de seguridad

Se ha decidido que, en caso de que se produzca una violación de seguridad, la interfaz se debe desactivar. Introducir el siguiente comando para hacer que la acción de seguridad sea la desactivación:

```
Sw1n1p1(config-if)#switchport port-security violation shutdown
```

Paso 11 Reactivar el puerto

Si se produce una violación de seguridad y el puerto se desconecta, use el comando *no shutdown* en la interfaz desactivada para reactivarlo.

```
Sw1n1p1(config-if)#no shutdown
```

Paso 12 Cambiar los parámetros de seguridad

Introducir el siguiente comando para verificar la tabla mac-address-table.

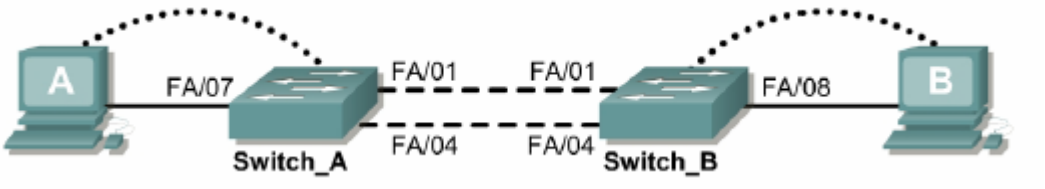
```
Sw1n1p1#show mac-address-table
```

Elimine la seguridad de puerto de la interfaz Fast Ethernet 0/4 de la siguiente manera:

```
Sw1n1p1(config)#interface gigabiteethernet 0/4
Sw1n1p1(config-if)#no switchport port-security
Sw1n1p1(config-if)#no switchport port-security mac-address sticky
Sw1n1p1(config-if)#no switchport port-security mac-address sticky (MAC-address)
Sw1n1p1(config-if)#shutdown
Sw1n1p1(config-if)#no shutdown
```

5.4 Practica 4. Selección del Puente Raíz

Figura 36. Grafica de guía para la prácticas 4.



Fuente. CCNA 3: Principio básicos de conmutación y enrutamiento intermedio v3.1 Manual de laboratorio para el estudiante

Tabla 10. Tabla de configuración de la practica 4.

Designación del *switch*	Nombre del *switch*	Contraseña enable secret	Contraseñas enable, de VTY y de Consola	Dirección IP de VLAN 1	IP del Gateway por defecto	Mascara de subred
Switch 1	Sw1n1p1	Class	SYC	10.10.250.2	10.10.250.1	255.255.255.0
Switch 2	Sw2n1p1	Class	SYC	10.10.250.3	10.10.250.1	255.255.255.0

AUTOR

Paso 1 Mostrar la tabla de Spanning-tree en cada *switch*

En la petición de entrada del modo EXEC privilegiado, escribir lo siguiente en el Sw1n1p1:

Sw1n1p1#**show spanning-tree brief**

En el Sw2n1p1, escriba el comando show spanning-tree brief en la petición de entradadel modo EXEC privilegiado como se indica a continuación:

Sw2n1p1#**show spanning-tree brief**

Con este comando se identifica cual es *switch* raíz, la prioridad y el id del puente raíz.

Paso 2 Reasignar el puente raíz

Se ha determinado que el *switch* que se ha seleccionado como puente raíz, utilizando los valores por defecto, no es la mejor opción. Es necesario obligar al "otro" *switch* a que se transforme en el *switch* raíz.
Como ejemplo, el *switch* raíz por defecto es el Sw1n1p1. Se prefiere usar al Sw2n1p1 como *switch* raíz. Si es necesario, vaya a la consola e introduzca el modo de configuración:
Determinar los parámetros que se pueden configurar para el Protocolo Spanning-Tree:

```
Sw2n1p1(config)#spanning-tree ?
Sw2n1p1(config)#spanning-tree vlan 1 priority 4096
Sw2n1p1(config)#exit
```

Paso 8 Mostrar la tabla de Spanning-tree del *switch*

En la petición de entrada del modo EXEC privilegiado, escriba lo siguiente en el Sw1n1p1:

```
Sw1n1p1#show spanning-tree brief
```

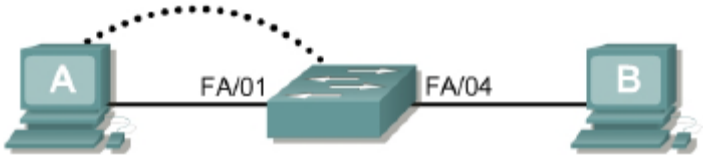
En el Sw2n1p1, escriba el comando show spanning-tree brief en la petición de entrada del modo EXEC privilegiado como se indica a continuación:

```
Sw2n1p1#show spanning-tree brief
```

Con el cambio de prioridad en el *switch* Sw2n1p1, el *switch* raíz, su prioridad y el id cambio.

5.5 Practica 5. Configuración VLAN estáticas

Figura 37. Grafica de guía para la prácticas 5.



Fuente. CCNA 3: Principio básicos de conmutación y enrutamiento intermedio v3.1 Manual de laboratorio para el estudiante

Tabla 11. Tabla de configuración de la practica 5.

Designación del *switch*	Nombre del *switch*	Contraseña enable secret	Contraseñas enable, de VTY y de Consola	Dirección IP de VLAN 1	IP del Gateway por defecto	Mascara de subred
Switch 1	Sw1n1p1	Class	SYC	10.10.250.2	10.10.250.1	255.255.255.0

AUTOR

Paso 1 Mostrar la información de la interfaz VLAN

En el Sw1n1p1, escribir el comando show VLAN en la petición de entrada del modo EXEC privilegiado:

```
Sw1n1p1#show vlan
```

Paso 2 Crear y otorgar un nombre a dos VLAN

Introducir los siguientes comandos para crear y otorgar un nombre a dos VLAN:

```
Sw1n1p1#vlan database
Sw1n1p1(vlan)#vlan 2 name VLAN2
Sw1n1p1(vlan)#vlan 3 name VLAN3
Sw1n1p1(vlan)#exit
```

Paso 3 Asignar puertos a VLAN 2

La asignación de puertos a las VLAN se debe realizar desde el modo de interfaz. Introducir los siguientes comandos para agregar el puerto 2 a la VLAN 2:

Sw1n1p1#**configure terminal**
Sw1n1p1(config)#**interface gigabiteethernet 0/2**
Sw1n1p1(config-if)#***switch*port mode access vlan 2**
Sw1n1p1(config-if)#**end**

Sw1n1p1#**configure terminal**
Sw1n1p1(config)#**interface gigabiteethernet 0/4**
Sw1n1p1(config-if)#***switch*port mode access vlan 3**
Sw1n1p1(config-if)#**end**

Paso 3 Eliminar un host de una VLAN

Para borrar un host de una VLAN, hay que ejecutar la forma no de los comandos *switch*port en el modo de configuración de interfaz de puerto.

Sw1n1p1#**configure terminal**
Sw1n1p1(config)#**interface gigabiteethernet 0/2**
Sw1n1p1(config-if)#**no *switch*port access vlan 2**

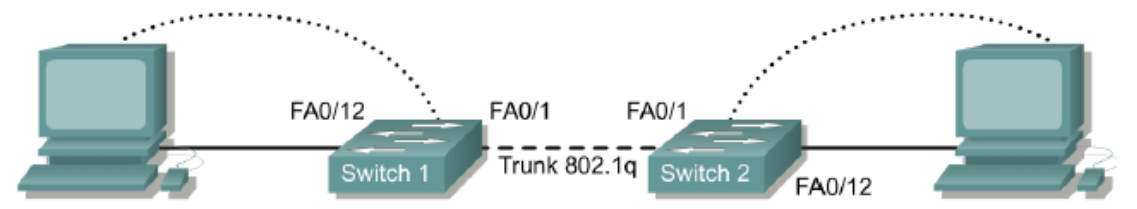
Paso 4 Eliminar una VLAN

Para borrar toda una VLAN, introducir el modo de base de datos de VLAN y ejecute la forma negativa del comando.

Sw1n1p1#**vlan database**
Sw1n1p1(vlan)#**no vlan 3**
Deleting VLAN 3
Sw1n1p1(vlan)#**exit**

5.6 Practica 6. Enlace troncal con 802.q

Figura 38. Grafica de guía para las prácticas 6 y 7.



Fuente. CCNA 3: Principio básicos de conmutación y enrutamiento intermedio v3.1 Manual de laboratorio para el estudiante

Tabla 12. Tabla de configuración de la práctica 6 y 7.

Designación del *switch*	Nombre del *switch*	Contraseña enable secret	Contraseñas enable, de VTY y de Consola	Dirección IP de VLAN 1	Mascara de subred	Nombres y números de VLAN
Switch 1	Sw1n1p1	Class	SYC	10.10.250.2	255.255.255.0	VLAN 1 Nativa VLAN 10 contabilidad VLAN 20 mercadeo VLAN 30 ingeniería
Switch 2	Sw2n1p1	Class	SYC	10.10.250.3	255.255.255.0	VLAN 1 Nativa VLAN 10 contabilidad VLAN 20 mercadeo VLAN 30 ingeniería

AUTOR

Paso 1 Crear y otorgar nombres a tres VLAN

Introducir los siguientes comandos para crear y otorgar nombres a tres VLAN:

Sw1n1p1#**vlan database**
Sw1n1p1(vlan)#**vlan 10 name contabilidad**
Sw1n1p1(vlan)#**vlan 20 name mercadeo**
Sw1n1p1(vlan)#**vlan 30 name ingenieria**
Sw1n1p1(vlan)#**exit**

Paso 2 Asignar puertos a una VLAN 10

La asignación de puertos a las VLAN se debe realizar desde el modo de interfaz. Introducir los siguientes comandos para agregar los puertos 0/4 al 0/6 a la VLAN 10:

```
Sw1n1p1#configure terminal
Sw1n1p1(config)#interface gigabiteethernet 0/4
Sw1n1p1(config-if)#switchport mode access
Sw1n1p1(config-if)#switchport access vlan 10
Sw1n1p1(config-if)#interface gigabiteethernet 0/5
Sw1n1p1(config-if)#switchport mode access
Sw1n1p1(config-if)#switchport access vlan 10
Sw1n1p1(config-if)#interface gigabiteethernet 0/6
Sw1n1p1(config-if)#switchport mode access
Sw1n1p1(config-if)#switchport access vlan 10
Sw1n1p1(config-if)#end
```

Paso 3 Asignar puertos a VLAN 20

Introducir los siguientes comandos para agregar los puertos 0/7 al 0/9 a la VLAN 20:

```
Sw1n1p1#configure terminal
Sw1n1p1(config)#interface gigabiteethernet 0/7
Sw1n1p1(config-if)#switchport mode access
Sw1n1p1(config-if)#switchport access vlan 20
Sw1n1p1(config-if)#interface gigabiteethernet 0/8
Sw1n1p1(config-if)#switchport mode access
Sw1n1p1(config-if)#switchport access vlan 20
Sw1n1p1(config-if)#interface gigabiteethernet 0/9
Sw1n1p1(config-if)#switchport mode access
Sw1n1p1(config-if)#switchport access vlan 20
Sw1n1p1(config-if)#end
```

Paso 4 Asignar puertos a VLAN 30

Introducir los siguientes comandos para agregar los puertos 0/10 al 0/12 a la VLAN 30:

```
Sw1n1p1#configure terminal
Sw1n1p1(config)#interface gigabiteethernet 0/10
```

Sw1n1p1(config-if)#***switch*port mode access**
Sw1n1p1(config-if)#***switch*port access vlan 30**
Sw1n1p1(config-if)#**interface gigabiteethernet 0/11**
Sw1n1p1(config-if)#***switch*port mode access**
Sw1n1p1(config-if)#***switch*port access vlan 30**
Sw1n1p1(config-if)#**interface gigabiteethernet 0/12**
Sw1n1p1(config-if)#***switch*port mode access**
Sw1n1p1(config-if)#***switch*port access vlan 30**
Sw1n1p1(config-if)#**end**

Paso 4 Crear y asignar los puertos al *switch* 2

Seguir los pasos 1,2 y 3 para el *switch* 2.

Paso 5 Crear el enlace troncal DOT1Q

En ambos *switches*, Sw1n1p1 y Sw2n1p1, escribir el siguiente comando en la petición de entrada del comando de la interfaz gigabiteethernet 0/1.

Sw1n1p1(config)#**interface gigabiteethernet 0/1**
Sw1n1p1(config-if)#***switch*port mode trunk**
Sw1n1p1(config-if)#***switch*port trunk encapsulation dot1q**
Sw1n1p1(config-if)#**end**

Sw2n1p1(config)#**interface gigabiteethernet 0/1**
Sw2n1p1(config-if)#***switch*port mode trunk**
Sw2n1p1(config-if)#***switch*port trunk encapsulation dot1q**
Sw2n1p1(config-if)#**end**

Paso 6 Verificar el enlace troncal DOT1Q

Para verificar que el puerto gigabiteethernet 0/1 se ha establecido como el puerto de enlace troncal, escriba show interface gigabiteethernet 0/1 *switch*port en el indicador de modo EXEC privilegiado.

Sw1n1p1#**show interface gigabiteethernet 0/1 *switch*port**

Sw2n1p1#**show interface gigabiteethernet 0/1 *switch*port**

Paso 7 Probar las VLAN y el enlace troncal

Hacer ping desde el host en el puerto 0/4 del Sw1n1p1 al host en el puerto 0/5 del Sw2n1p1, que pertenecen a la misma VLAN.

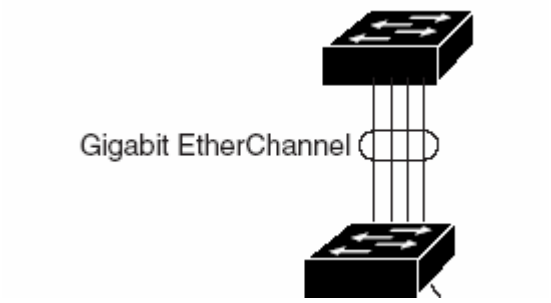
Hacer ping desde el host en el puerto 0/7 del Sw1n1p1 al host en el puerto 0/8 del Sw2n1p1, que pertenecen a la misma VLAN.

Hacer ping desde el host en el puerto 0/10 del Sw1n1p1 al host en el puerto 0/11 del Sw2n1p1, que pertenecen a la misma VLAN.

Paso 8 configurar un port-channel

En ambos *switches*, Sw1n1p1 y Sw2n1p1, escriba el siguiente comando en la petición de entrada del comando de la interfaz gigabiteethernet 0/1 y 0/2.

Figura 39. Port-Channel



Sw1n1p1#**configure terminal**
Sw1n1p1(config)#**interface range gigabitethernet0/1 -2**
Sw1n1p1(config-if-range)#***switch*port mode access**
Sw1n1p1(config-if-range)#***switch*port access vlan 1**
Sw1n1p1(config-if-range)#**channel-group 1 mode desirable non-silent**
Sw1n1p1(config-if-range)#**end**

Sw2n1p1#**configure terminal**
Sw2n1p1(config)#**interface range gigabitethernet0/1 -2**
Sw2n1p1(config-if-range)#***switch*port mode access**
Sw2n1p1(config-if-range)#***switch*port access vlan 1**
Sw2n1p1(config-if-range)#**channel-group 1 mode desirable non-silent**
Sw2n1p1(config-if-range)#**end**

Paso 9 Probar las VLAN y el enlace port-channel

Hacer ping desde el host en el puerto 0/4 del Sw1n1p1 al host en el puerto 0/5 del Sw2n1p1, que pertenecen a la misma VLAN.

Hacer ping desde el host en el puerto 0/7 del Sw1n1p1 al host en el puerto 0/8 del Sw2n1p1, que pertenecen a la misma VLAN.

Hacer ping desde el host en el puerto 0/10 del Sw1n1p1 al host en el puerto 0/11 del Sw2n1p1, que pertenecen a la misma VLAN.

Desconectar el puerto 0/1 de cualquiera de los dos *switches* y volver a repetir los pings en donde tienen que ser exitosos ya que el enlace es un port-channel y no detecta ningún cambio si desconecta uno de los dos puertos que lo conforma.

5.7 Practica 7. Configuración de servidor y cliente VTP

Para esta práctica, la topología usada se encuentra en la figura 38.

Paso 1 Configurar VTP

Se debe configurar el protocolo de enlace troncal virtual (VTP) en ambos *switches*. VTP es el protocolo que comunica información acerca de cuáles son las VLAN que existen de un *switch* a otro. Si VTP no suministra esta información, las VLAN deberían crearse en todos los *switches* de forma individual.

Por defecto, los *switches* de la serie Catalyst se configuran como servidores VTP. En caso de que los servicios del servidor se desactiven, se usa el siguiente comando en el Sw1n1p1 para reactivarlos.

```
Sw1n1p1#vlan database
Sw1n1p1(vlan)#vtp server
Sw1n1p1(vlan)#vtp domain group1
Sw1n1p1(vlan)#exit
```

Paso 2 Crear y otorgar nombres a tres VLAN

Introducir los siguientes comandos para crear y otorgar un nombre a tres VLAN:

```
Sw1n1p1#vlan database
Sw1n1p1(vlan)#vlan 10 name contabilidad
Sw1n1p1(vlan)#vlan 20 name mercadeo
Sw1n1p1(vlan)#vlan 30 name ingenieria
Sw1n1p1(vlan)#exit
```

Paso 3 Configurar cliente VTP

Introducir los siguientes comandos para configurar el Sw2n1p1 para que funcione como cliente VTP:

```
Sw2n1p1#vlan database
Sw2n1p1(vlan)#vtp client
Sw2n1p1(vlan)#vtp domain group1
Sw2n1p1(vlan)#exit
```

Paso 4 Crear el enlace troncal

En ambos *switches*, Sw1n1p1 y Sw2n1p1, escribir el siguiente comando en la petición de entrada de comandos de la interfaz gigabiteethernet 0/1. Observe que no es necesario especificar el encapsulamiento en un 2960G, dado que sólo admite 802.1Q.

```
Sw1n1p1(config)#interface gigabiteethernet 0/1
Sw1n1p1(config-if)#switchport mode trunk
Sw1n1p1(config-if)#end

Sw2n1p1(config)#interface gigabiteethernet 0/1
Sw2n1p1(config-if)#switchport mode trunk
Sw2n1p1(config-if)#end
```

Paso 5 Mostrar la información de la interfaz VLAN

En el Sw2n1p1, escriba el comando show vlan en el modo EXEC privilegiado, el protocolo VTP debe copiar las misma cofiguracion de VLAN que tiene el Sw1n1p1 en el Sw2n1p1:

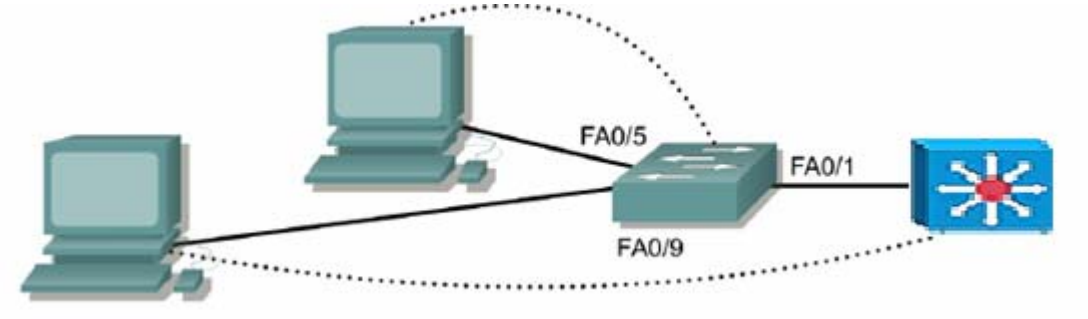
```
Sw2n1p1#show vlan
```

Paso 6 Probar las VLAN y el enlace troncal

Hacer ping desde el host en un puerto del Sw1n1p1 al host de un puerto del Sw2n1p1, que pertenecen a la misma VLAN.

5.8 Practica 8. Configuración de enrutamiento entre VLAN

Figura 40. Grafica de guía para la práctica 8.



Fuente. CCNA 3: Principio básicos de conmutación y enrutamiento intermedio v3.1 Manual de laboratorio para el estudiante

Tabla 13. Tabla de configuración de la practica 8.

Designación del *switch*	Nombre del *switch*	Contraseña enable secret	Contraseñas enable, de VTY y de Consola	Dirección IP de VLAN	Mascara de subred
Switch 1	Sw1n1p1	Class	SYC		
Switch 2 (capa3)	Sw2n1p1	Class	SYC	VLAN 10: 10.10.100.1 VLAN 20: 10.10.200.1	255.255.255.0

AUTOR

Paso 1 Configurar los hosts conectados al *switch*

Configurar los hosts utilizando la siguiente información.

Para el host en el puerto 0/5:
Dirección IP 10.10.100.5
Máscara de subred 255.255.255.0
Gateway por defecto 10.10.100.1

Para el host en el puerto 0/9:
Dirección IP 10.10.200.1
Máscara de subred 255.255.255.0
Gateway por defecto 10.10.200.1

Paso 2 Crear y otorgar nombres a dos VLAN

Introduzca los siguientes comandos para crear y otorgar nombres a dos VLAN

```
Sw1n1p1#vlan database
Sw1n1p1(vlan)#vlan 10 name compras
Sw1n1p1(vlan)#vlan 20 name soporte
Sw1n1p1(vlan)#exit
```

Paso 3 Asignar puerto a VLAN 10

La asignación de puertos a las VLAN se debe realizar desde el modo de interfaz. Introduzca los siguientes comandos para agregar el puertos 0/5 a la VLAN 10:

```
Sw1n1p1#configure terminal
Sw1n1p1(config)#interface gigabiteethernet 0/5
Sw1n1p1(config-if)#switchport mode access
Sw1n1p1(config-if)#switchport access vlan 10
Sw1n1p1(config-if)#end
```

Paso 4 Asignar puertos a VLAN 20

Introducir los siguientes comandos para agregar el puerto 0/9 a la VLAN 20:

```
Sw1n1p1#configure terminal
Sw1n1p1(config)#interface gigabiteethernet 0/9
Sw1n1p1(config-if)#switchport mode access
Sw1n1p1(config-if)#switchport access vlan 20
Sw1n1p1(config-if)#end
```

Paso 5 Mostrar la información de la interfaz VLAN

En el Sw1n1p1, escribir el comando show vlan en el modo EXEC privilegiado:

```
Sw1n1p1#show vlan
```

Paso 6 Crear el enlace troncal

En el Sw1n1p1 y Sw2n1p1, escribir los siguientes comandos en la petición de entrada de la interfaz GigabiteEthernet 0/1.

Sw1n1p1(config)#**interface gigabiteethernet0/1**
Sw1n1p1(config-if)#***switch*port mode trunk**
Sw1n1p1(config-if)#**end**

Sw2n1p1(config)#**interface gigabiteethernet0/1**
Sw2n1p1(config-if)#***switch*port mode trunk**
Sw2n1p1(config-if)#***switch*port trunk encapsulation dot1q**
Sw2n1p1(config-if)#**end**

Paso 7 Configurar el *switch* de capa 3 para el enrutamiento

Configure el Sw2n1p1 con los siguientes datos.

Sw2n1p1#**configure terminal**
Sw2n1p1#**ip routing**
Sw2n1p1#**end**

Sw2n1p1#**vlan database**
Sw2n1p1(vlan)#**vlan 10 name compras**
Sw2n1p1(vlan)#**vlan 20 name soporte**
Sw2n1p1(vlan)#**exit**

Sw2n1p1(config)#**interface VLAN 10**
Sw2n1p1(config-if)#**ip address 10.10.100.1 255.255.255.0**
Sw2n1p1(config-if)#**exit**

Sw2n1p1(config)#**interface VLAN 20**
Sw2n1p1(config-if)#**ip address 10.10.200.1 255.255.255.0**
Sw2n1p1(config-if)#**exit**

Paso 8 Verificar las rutas conectadas en el Sw2n1p1

Escribir el siguiente comando para verificar las rutas conectadas directamente. Como las dos VLANs creadas están conectadad directamente en el mismo *switch* con solo habilitando el ip routing, el *switch* asume esas rutas dejando tener comunicación entre las VLANs creadas.

Sw1n1p1#**Show ip route**

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
Gateway of last resort is not set

C 10.10.100.0/24 is directly connected, Vlan10
C 10.10.200.0/24 is directly connected, Vlan20

Paso 9 Probar que las VLANS se vean

Hacer ping desde el host del puerto 0/5 al host del puerto 0/9.

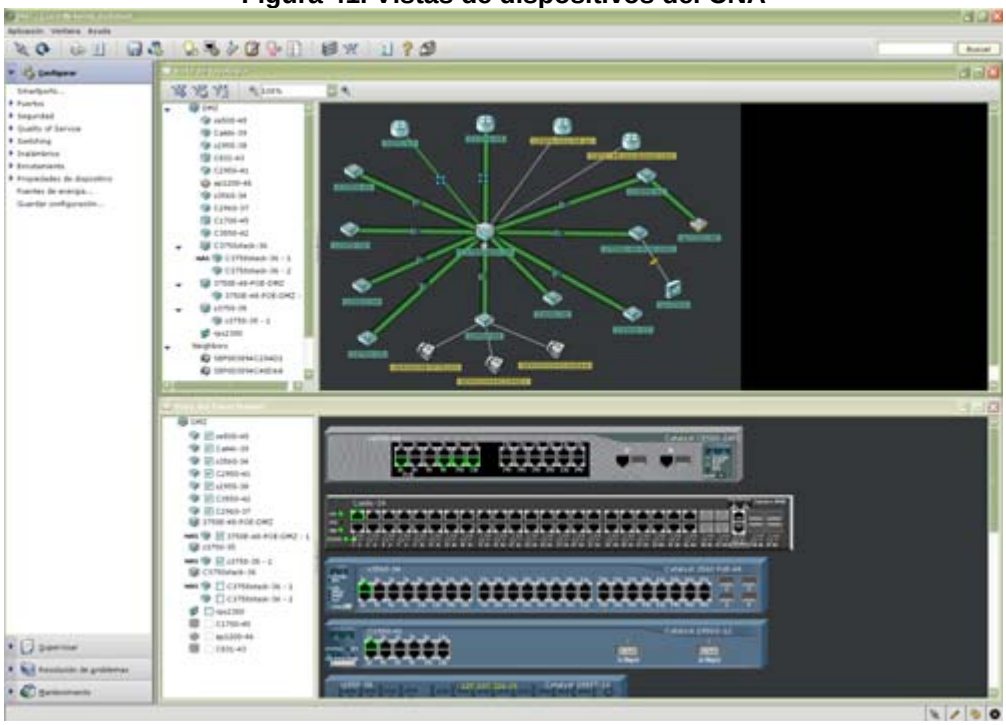
6 ANALISIS Y RESULTADOS

En esta sección se analiza el rendimiento de la red después del proyecto de reingeniería que se implemento a la infraestructura de SYC S.A. con el fin de verificar la correcta operación del sistema. Para esto la administración de la red se realiza por medio de un sistema de gestión instalado para tener control de todos los dispositivos de red que conforma la empresa.

El sistema de gestión que se implementó es el asistente de redes de CISCO, (CISCO Network Assistant, CNA), que es un software cuya aplicación se utiliza para administrar los dispositivos individuales y grupales, desde cualquier lugar de la Intranet.

Este sistema nos permite aplicar acciones a los dispositivos que conforman la red como generación de estadísticas y supervisión de enlaces. Como se puede observar en la figura 41, CNA ofrece 2 vistas de los dispositivos que conforman la red. La primera es una topología física de cómo esta conectados los dispositivos de red y la segunda una vista del panel frontal, donde es posible administrar en tiempo real los dispositivos.

Figura 41. Vistas de dispositivos del CNA



Fuente. Guía de inicio de Cisco Network Assistant Versión 5.1

Como anteriormente se escribió este sistema de gestión se instalo para realizar la administración de la red, donde exige crear una comunidad, que es un grupo de dispositivos de red, que por medio del protocolo de descubrimiento de CISCO (CISCO Protocol discovery, CDP), protocolo creado para dispositivos CISCO, encuentra los dispositivos de la red agregándolos a la comunidad y así efectuar su respectiva administración.

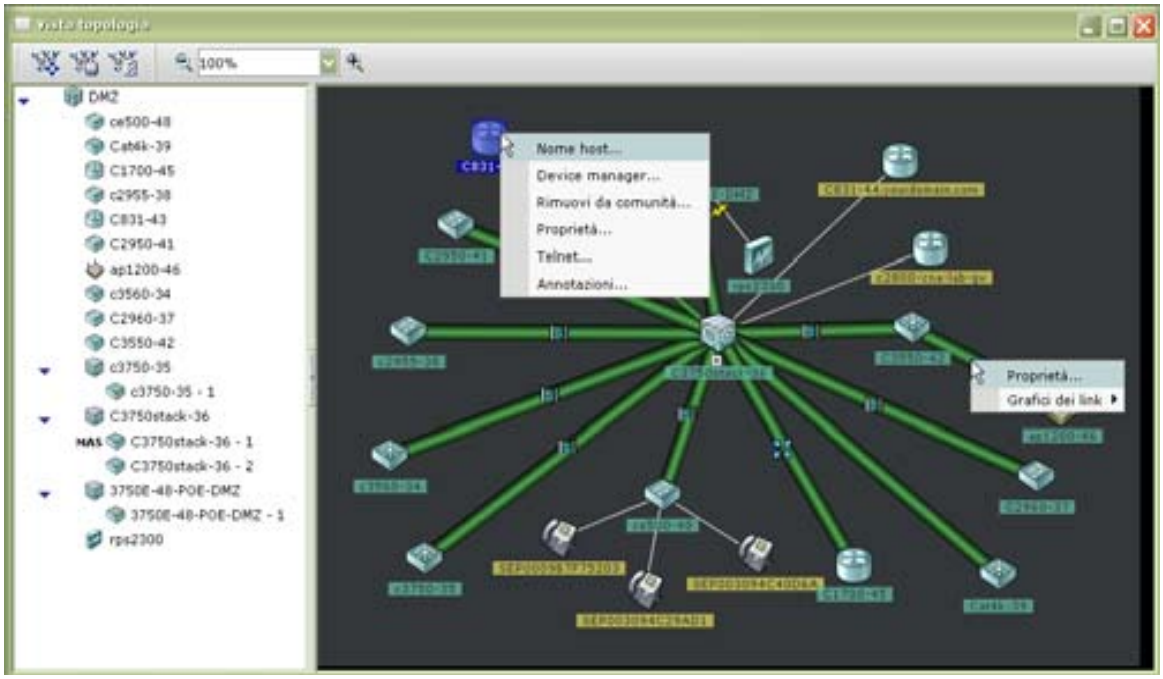
6.1 CISCO NETWORK ASSISTANT (CNA)

Esta sección describe las pautas, requisitos y advertencias que se tuvieron en cuenta para crear la comunidad DG.SYC en el sistema de gestión.
Para esto se tuvo en cuenta que todos los dispositivos de red que conforman la empresa tuvieran dirección IP. La dirección usada se explicó anteriormente en la sección 4.3.3 Diseño e implementación de la capa 3. Donde se uso la sub red 10.10.250.0 para el manejo de los dispositivos de red.

Para la creación de la comunidad se le pidió al sistema de gestión CNA, que detectara los dispositivos con la dirección 10.10.250.1 – 10.10.250.254, descubriendo así todos los *switches* que conforman la empresa. Como resultado, CNA muestra la topología física de la red empresarial, la cual se pudo observar en la figura 28.

Una vez creada la comunidad, CNA deja administrar de varias maneras a los dispositivos que la conforman. La forma utilizada para administrar la red, fue por medio de la comunicación por acceso remoto más conocida como Telnet (Telecomunication Network), que sirve para acceder mediante una red a otra máquina para manejarla como si estuviéramos sentados delante de ella. La figura 42 muestra una ventana de funciones del la cual hace parte Telnet como función de administración para acceder al dispositivo. El puerto que usa Telnet es el 23. Uno de los métodos para probar el buen funcionamiento de red en todas las capas del modelo OSI, es haciendo uso de Telnet, si la conexión es efectiva se prueba que la comunicación de red esta 100 % disponible.

Figura 42. Administración de dispositivo de red



Fuente. Guía de inicio de Cisco Network Assistant Versión 5.1

6.2 MEDICION DE LA UTILIZACION DEL ANCHO DE BANDA DE LOS DISPOSITIVOS QUE CONFORMAN EL BACKBONE EMPRESARIAL

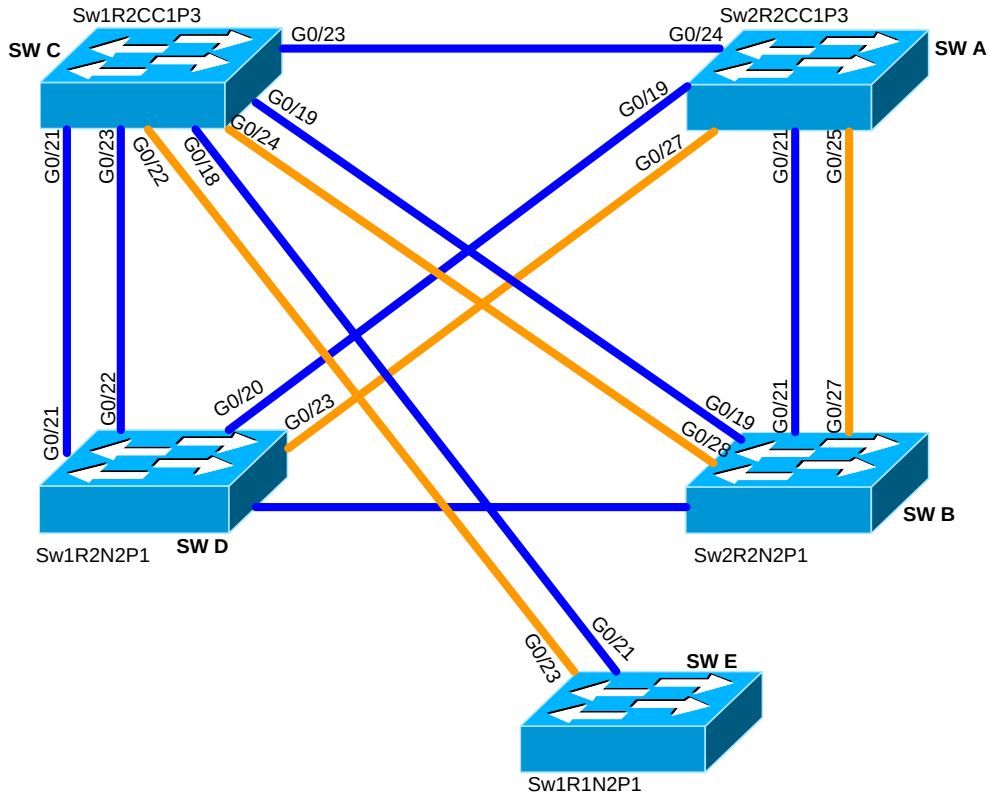
El objetivo de estas estadísticas es de medir la utilización del ancho de banda interno de cada uno de los 5 *switches* que conforma el backbone de la red empresarial. Esto quiere decir la utilización completa de todos los puertos que conforma el *switch*. Las siguientes graficas fueron tomadas un día entre semana en el mes de junio por medio del sistema de gestión CNA, en un intervalo de tiempo que va desde las 4 pm hasta las 6 pm, horas que pueden ser críticas en los procesos de producción de la empresa.

En la figura 43 encontramos la topología de los 5 *switches* que conforman el backbone de la red empresarial con sus respectivos enlaces. Las figuras 43 – 47, son las graficas de utilización del ancho de banda del *switch* A – E respectivamente. Cada una de las graficas fue tomada a horas distintas. El SW A es el principal de los 5 *switches* del backbone, ya que este es el *switch*

de capa 3 donde hace la función de ruteo de toda la red empresarial. La estadística de tiempo de la grafica 43 del *switch* A corresponde a las 4 pm siendo así la hora de la tarde mas critica en la producción de la empresa.

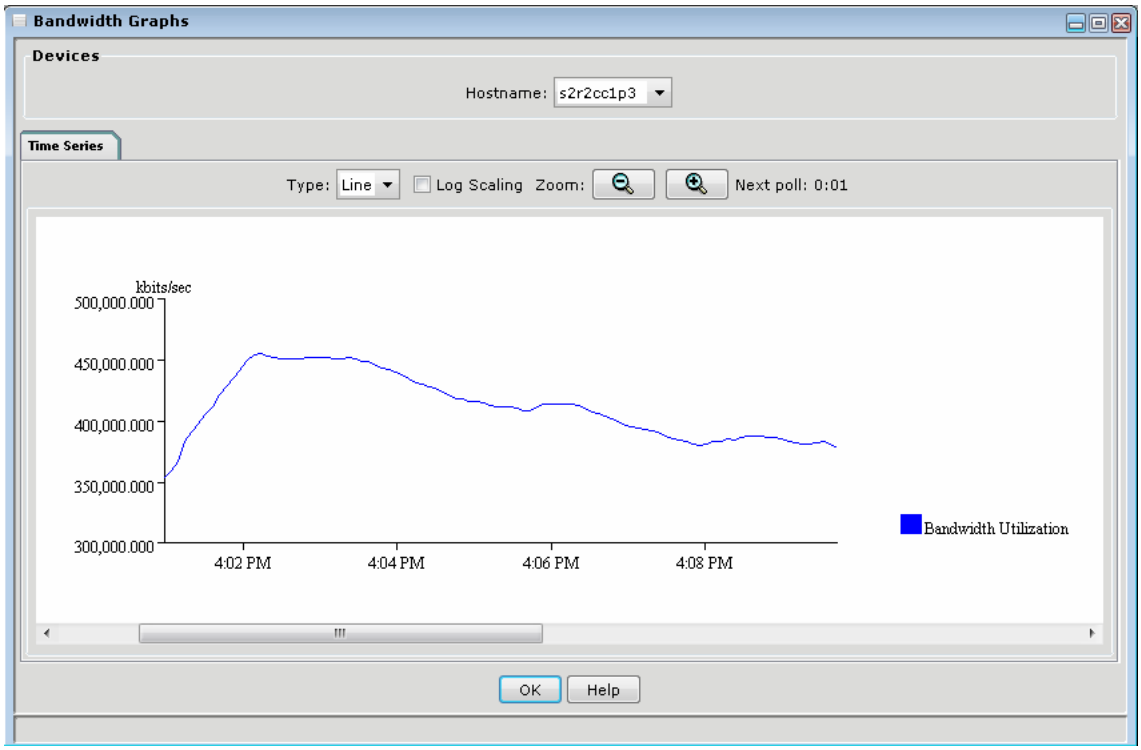
Como era de esperarse por las características que presenta el *switch* en la red empresarial fue la estadística más alta con respecto al rendimiento de la utilización del ancho de banda total del *switch* con respecto a los demás *switches*. Como se dijo anteriormente estas estadísticas corresponde a toda la sumatoria de puertos y uso de memoria total del *switch*, se tiene en cuenta que cada *switch* CISCO catalyst 2960G tiene 24 puertos y el 3560G tiene 28 puertos, de los cuales pueden tener de 2 a 4 puertos para fibra óptica, en este caso utilizado para el backbone empresarial.

Figura 43. Backbone Red SYC



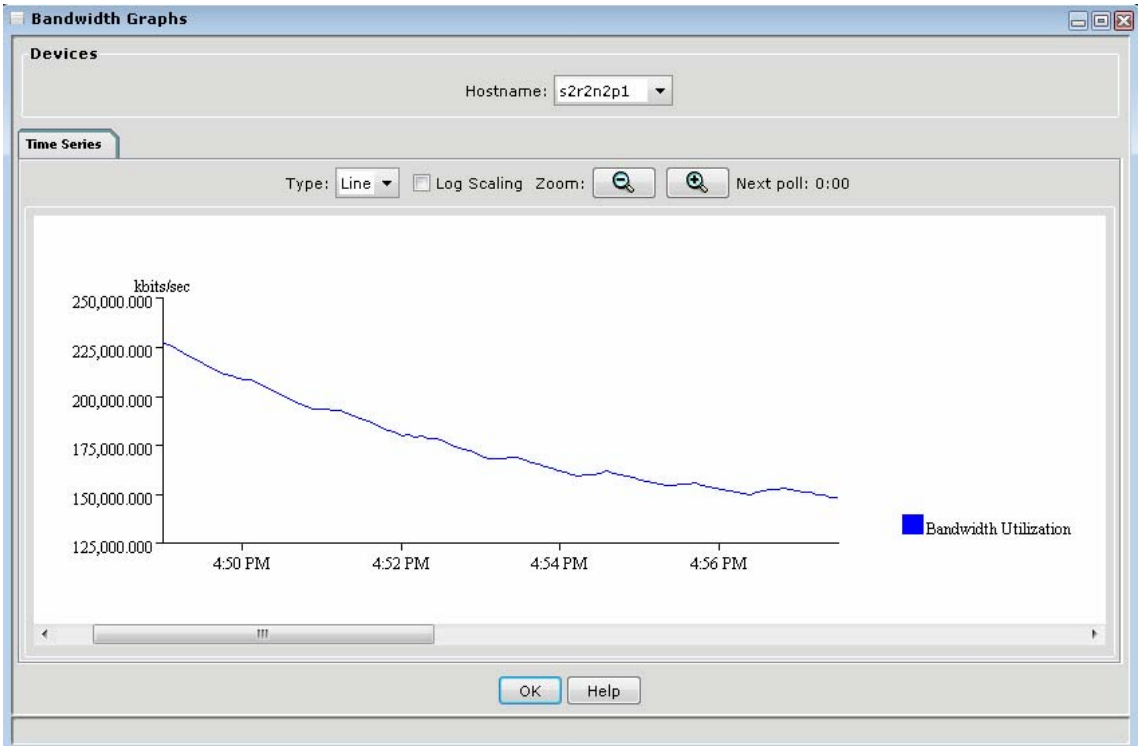
AUTOR

Figura 44. Utilización del ancho de banda del SW A (Sw2R2CC1P3)



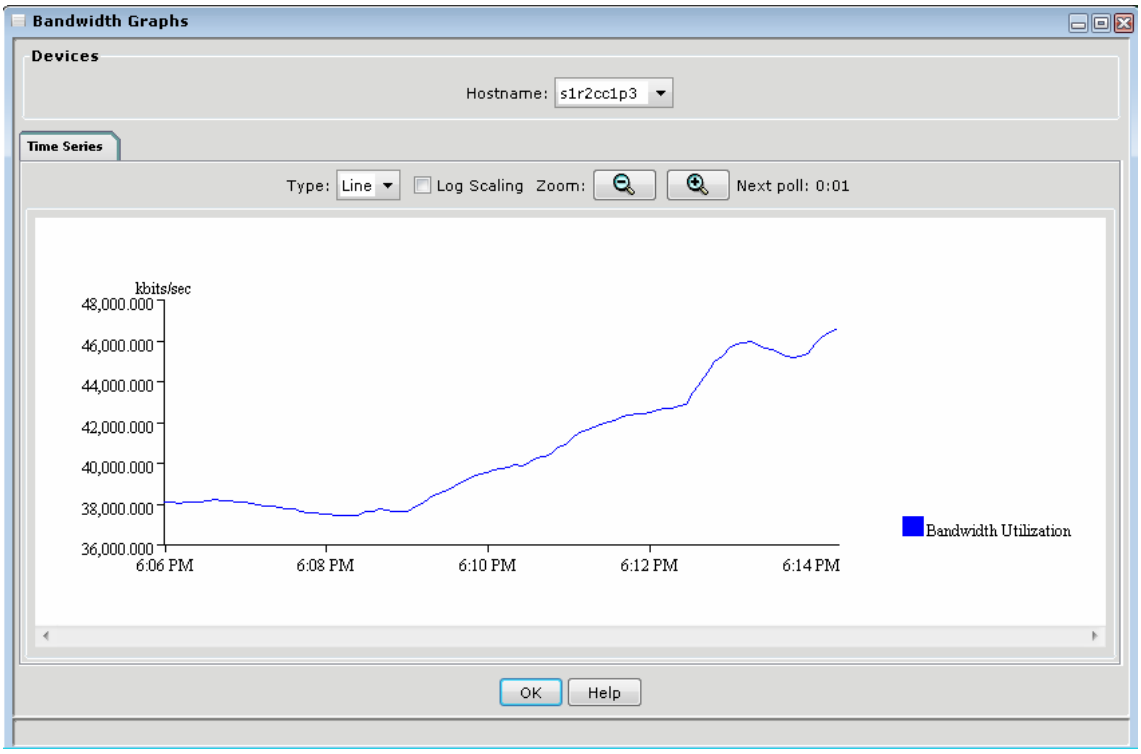
Fuente. CNA Red SYC S.A, Junio 2008

Figura 45. Utilización del ancho de banda del SW B (Sw2R2N2P1)



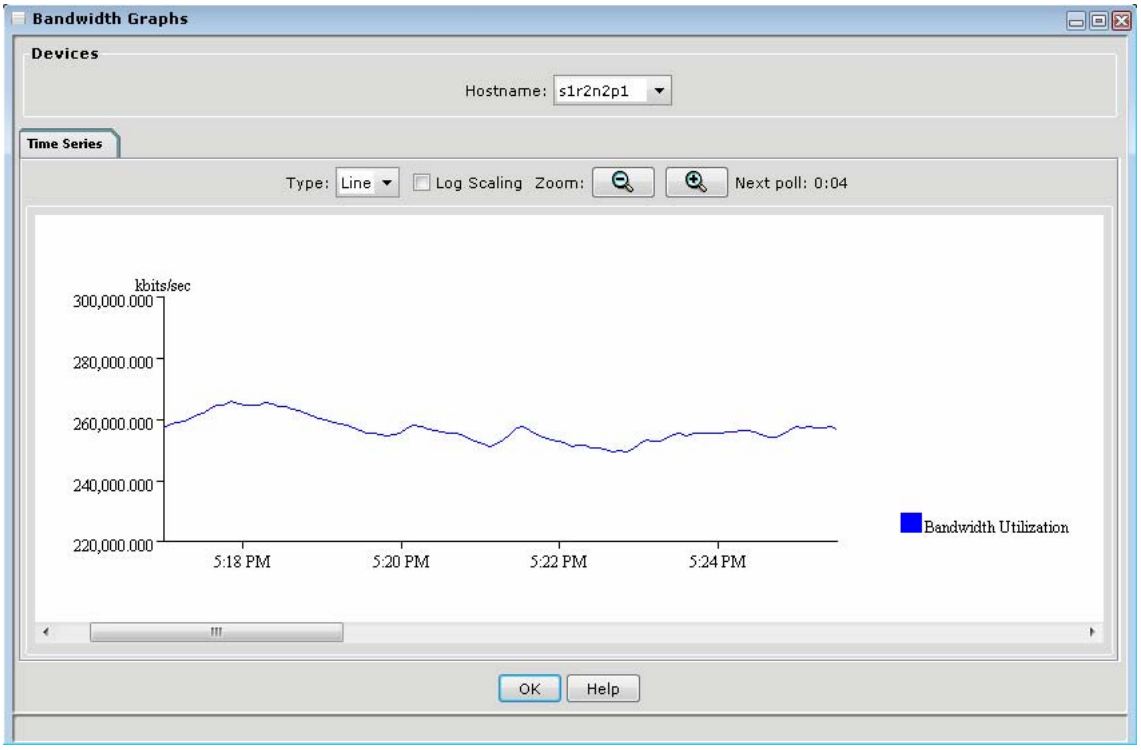
Fuente. CNA Red SYC S.A, Junio 2008

Figura 46. Utilización del ancho de banda del SW C (Sw1R2CC1P3)



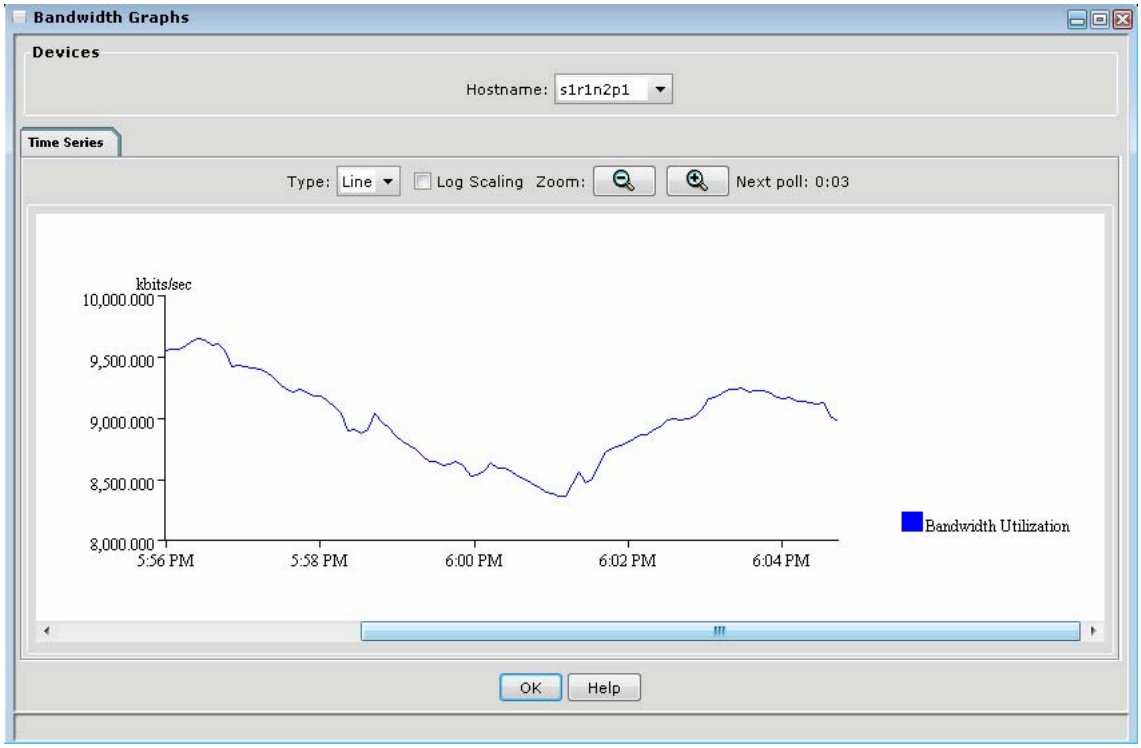
Fuente. CNA Red SYC S.A, Junio 2008

Figura 47. Utilización del ancho de banda del SW D (Sw1R2N2P1)



Fuente. CNA Red SYC S.A, Junio 2008

Figura 48. Utilización del ancho de banda del SW E (Sw1R1N2P1)



Fuente. CNA Red SYC S.A, Junio 2008

La tabla 11 es un resumen de las estadísticas de las figuras 43 – 48 donde menciona el máximos consumo en kbits/seg que presenta el *switch* con su respectiva hora.

Tabla 11. Consumo de tráfico de *switches* de backbone.

CONSUMO DE TRAFICO		
SWITCH	**MAX CONSUMO Kbits/seg**	**HORA**
SW A	450,000.000	4:02 PM
SW B	225,000.000	4:58 PM
SW C	46,000.000	6:14 PM
SW D	265,000.000	5:18 PM
SW E	9,500.000	5:56 PM

AUTOR

CONCLUSIONES

Para iniciar un proyecto de reingeniería de una red LAN empresarial, se tiene en cuenta el debido conocimiento que se tiene con los distintos dispositivos que se pueden manejar para el proyecto, seguido de un debido análisis de los problemas de la estructura de red que se presentan para así poder implementar las soluciones adecuadas siguiendo la respectivas etapas de diseño de una red LAN.

Para la implementación del re-diseño de la red LAN, se debe tener un dominio claro las capas de modelo OSI, especialmente las tres primeras capas (capa física, capa de enlace y capa de red), para que la red cumpla con los estándares y poder obtener el rendimiento adecuado que exige la red.

Como se observa en el proyecto de reingeniería se baso en el manejo de dispositivos de red de marca CISCO (en este caso los *switches* CISCO catalyst 2960G y 3560G), el cual se complemento los estudio de los sus distintos procedimientos de configuración con el curso de CISCO CCNA para así poderlos aplicar a la reingeniería de la infraestructura de la red LAN.

Los ingenieros a cargo del proyecto deben tener la capacidad de interpretar la necesidad y encontrar la mejor solución. También durante la implementación de la solución se debe tratar de tener el menor impacto posible durante el proceso de cambio, se tiene en cuenta que la empresa no para su producción.

Se plantea una solución sencilla, donde se empieza con el análisis de red LAN que tenia la empresa, identificando los problemas de red y realizando un re diseño de la red con base a las soluciones planteadas.

El re diseño de la red LAN establece para cada proyecto o grupo organizativo de la empresa, un espacio totalmente independiente, con garantías de velocidad y buen ancho de banda, esto se da gracias a los dispositivos de red

de capa 2 (*switches* CISCO 2960G), utilizados en la infraestructura de red de este proyecto.

La utilización de redes de área local virtuales conocida como VLAN´s garantiza la independencia de los distintos segmentos de red que conforma la red LAN empresarial. El dispositivo de capa 3 (*switch* CISCO 3560G) permite la comunicación de las distintas VLAN´s de la red LAN garantizando así fluidez de datos entre todos los proyectos o grupos organizativos de la empresa. El uso de VLAN´s en el presente proyecto aumento el número y redujo el tamaño de *dominios de broadcast.*

Para la administración de la red LAN empresarial se utilizo el software CISCO NETWORK ASSISTANT (CNA, Asistente de redes de CISCO), esta herramienta es utilizada para la administración de los dispositivos de red que conforma la empresa desde cualquier lugar de la intranet.

RECOMENDACIONES

Para el desarrollo de un proyecto empresarial no solo se debe preparar para solucionar el problema presentado sino también realizar su implementación sin afectar el servicio que presenta la empresa, el cambio realizado debe tener el menor impacto posible donde se cuadran los días y las horas más acertadas para configurar equipos de red que pueden afectar con la producción.

La solución de red que se plantee para la empresa debe ser una solución integral, tanto en software como en hardware, esto le permitirá tener un mayor control en la administración y compatibilidad de los equipos.

El desarrollo de una red de datos para una empresa debe iniciar con una visita previa antes de la ejecución, para saber cuál es la infraestructura de red que posee o plantea la empresa, dejar claros los objetivos y requisitos que la empresa necesita para así plantear el diseño de red adecuado.

La empresa debe ser consciente que la solución de red deben tener siempre las siguientes características: la red debe ser funcional, escalable, adaptable y fácil de administrar. El promedio que debe durar una red antes de volver hacer una reingeniería es de 7 a 10 años.

BIBLIOGRAFIA

LIBROS

- Academia de Networking de Cisco Systems Guía del primer año CCNA 1 y 2 pág. 41
- Academia de Networking de Cisco Systems Guía del primer año CCNA 1 y 2 pág. 73
- Academia de Networking de Cisco Systems Guía del primer año CCNA 1 y 2 pág. 395
- Academia de Networking de Cisco Systems Guía del primer año CCNA 3 y 4 pág. 262
- Academia de Networking de Cisco Systems Guía del primer año CCNA 3 y 4 pág. 161
- Academia de Networking de Cisco Systems Guía del primer año CCNA 3 y 4 pág. 166
- Academia de Networking de Cisco Systems Guía del primer año CCNA 3 y 4 pág. 177-178
- Academia de Networking de Cisco Systems Guía del primer año CCNA 3 y 4 pág. 208
- Academia de Networking de Cisco Systems Guía del primer año CCNA 3 y 4 pág. 210
- Academia de Networking de Cisco Systems Guía del primer año CCNA 3 y 4 pág. 212
- Academia de Networking de Cisco Systems Guía del primer año CCNA 3 y 4 pág. 253
- Academia de Networking de Cisco Systems Guía del primer año CCNA 3 y 4 pág. 288 y 289
- Academia de Networking de Cisco Systems Guía del primer año CCNA 3 y 4 pág. 316

TUTORIALES.

- Principio básicos de conmutación y enrutamiento intermedio v3.1 Manual de laboratorio para el estudiante.
- Catalyst 2960 *Switch* Software Configuration Guide Cisco IOS Release 12.2(37)SE May 2007
- Catalyst 3560 *Switch* Software Configuration Guide Cisco IOS Release 12.1(19)EA1 January 2004
- Guía de inicio de Cisco Network Assistant Versión 5.1
- Catalyst 3750-E and 3560-E *Switch* Command Reference Cisco IOS Release 12.2(40)SE August 2007

SITIOS WEB RECOMENDADOS

- http://www.masadelante.com/faq-lan.htm
- http://es.wikipedia.org/wiki/Ethernet
- http://www.syc.com.co/
- http://es.wikipedia.org/wiki/1000BASE-X
- http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP
- http://www.almacen-informatico.com/CISCO_catalyst-2960g-24tc-WS-C2960G-24TC-L_32222_p.htm#extended_spec
- http://www.almacen-informatico.com/CISCO_catalyst-3560g-24ts-WS-C3560G-24TS-S_32334_p.htm
- http://www.eveliux.com/mx/index.php?option=content&task=view&id=151
- http://elisoft.comvive.com/docus/rfc1918.htm

ANEXO A.
Cisco Catalyst 2960G-24TC

Cisco Catalyst 2960G-24TC

Conmutador - 24 puertos - EN, Fast EN, Gigabit EN - 10Base-T, 100Base-TX, 1000Base-T + 4 x SFP compartido (vacías) - 1U - montable en bastidor

La familia Catalyst de Cisco es una completísima línea de *switches* de alto rendimiento diseñados para ayudar a los usuarios a que pasen de forma sencilla de las redes LAN compartidas tradicionales a redes completamente conmutadas. Los *switches* Catalyst de Cisco ofrecen un amplio espectro para aplicaciones de usuarios, desde *switches* para pequeños grupos de trabajo hasta *switches* multicapa para aplicaciones empresariales escalables en el centro de datos o en el backbone. Los *switches* Catalyst ofrecen rendimiento, administración y escalabilidad, se puede encontrar equipos Ethernet, Fast Ethernet y con opciones modulares las cuales permiten adaptarlos a las necesidades del negocio.

Información principal

Descripción del producto	Cisco Catalyst 2960G-24TC - conmutador - 24 puertos
Tipo de dispositivo	Conmutador
Factor de forma	Montable en bastidor - 1U
Dimensiones (Ancho x Profundidad x Altura)	44.5 cm x 32.8 cm x 4.4 cm
Peso	4.5 kg
Memoria RAM	64 MB
Memoria Flash	32 MB
Cantidad de puertos	24 x Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T
Velocidad de transferencia de datos	1 Gbps
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Ranuras vacías	4 x SFP compartido (mini-GBIC)
Protocolo de gestión remota	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP
Modo comunicación	Semidúplex, dúplex pleno
Características	Auto-sensor por dispositivo, soporte de DHCP, negociación automática, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), snooping IGMP
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah
Alimentación	CA 120/230 V (50/60 Hz)

Especificaciones ampliadas

General

Tipo de dispositivo	Conmutador
Tipo incluido	Montable en bastidor - 1U
Anchura	44.5 cm
Profundidad	32.8 cm
Altura	4.4 cm
Peso	4.5 kg

Memoria

Memoria RAM	64 MB
Memoria Flash	32 MB Flash

Conexión de redes

Cantidad de puertos	24 x Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T
Velocidad de transferencia de datos	1 Gbps
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Protocolo de gestión remota	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP
Tecnología de conectividad	Cableado
Modo comunicación	Semidúplex, dúplex pleno
Protocolo de conmutación	Ethernet
Tamaño de tabla de dirección MAC	8K de entradas
Indicadores de estado	Actividad de enlace, velocidad de transmisión del puerto, modo puerto duplex, alimentación, tinta OK, sistema
Características	Auto-sensor por dispositivo, soporte de DHCP, negociación automática, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), snooping IGMP
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah

Expansión / Conectividad

Total ranuras de expansión (libres)	4 (4) x SFP (mini-GBIC)
Interfaces	24 x red - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45

Diverso

Método de autentificación	RADIUS, TACACS+, Secure Shell v.2 (SSH2)
Cumplimiento de normas	CE, TUV GS, cUL, EN 60950, EN55022, NOM, VCCI Class A ITE, IEC 60950, EN55024, FCC Part 15, UL 1950 Third Edition, CSA 22.2 No. 950 Third Edition

Alimentación

Dispositivo de alimentación	Fuente de alimentación - interna
Voltaje necesario	CA 120/230 V (50/60 Hz)
Consumo eléctrico en funcionamiento	75 vatios
Características	Contector de sistema de alimentación redundante (RPS)

Accesorios

Cables de sistema y alimentación	
CAB-JPN-RA=	Cisco - Cable de alimentación
Adaptadores de red	
GLC-LH-SM=	Cisco - Módulo de transceptor - SFP - Gigabit EN - 1000Base-LX, 1000Base-LH - 1300 nm
CWDM-SFP-1590=	Cisco CWDM SFP - Módulo de transceptor - SFP - Gigabit EN, 2Gb Fibre Channel - CWDM - 1590 nm
CWDM-SFP-1550=	Cisco CWDM SFP - Módulo de transceptor - SFP - Gigabit EN, 2Gb Fibre Channel - CWDM - 1550 nm
GLC-SX-MM=	Cisco - Módulo de transceptor - SFP - Gigabit EN - 1000Base-SX - 850 nm
CWDM-SFP-1490=	Cisco CWDM SFP - Módulo de transceptor - SFP - Gigabit EN, 2Gb Fibre Channel - CWDM - 1490 nm
CWDM-SFP-1510=	Cisco CWDM SFP - Módulo de transceptor - SFP - Gigabit EN, 2Gb Fibre Channel - CWDM - 1510 nm
CWDM-SFP-1470=	Cisco CWDM SFP - Módulo de transceptor - SFP - Gigabit EN, 2Gb Fibre Channel - CWDM - 1470 nm

ANEXO B.
Cisco Catalyst 3560G-24TS

Cisco Catalyst 3560G-24TS

Conmutador - 24 puertos - EN, Fast EN, Gigabit EN - 10Base-T, 100Base-TX, 1000Base-T + 4 x SFP (vacías) - 1U

La familia Catalyst de Cisco es una completísima línea de *switches* de alto rendimiento diseñados para ayudar a los usuarios a que pasen de forma sencilla de las redes LAN compartidas tradicionales a redes completamente conmutadas. Los *switches* Catalyst de Cisco ofrecen un amplio espectro para aplicaciones de usuarios, desde *switches* para pequeños grupos de trabajo hasta *switches* multicapa para aplicaciones empresariales escalables en el centro de datos o en el backbone. Los *switches* Catalyst ofrecen rendimiento, administración y escalabilidad, se puede encontrar equipos Ethernet, Fast Ethernet y con opciones modulares las cuales permiten adaptarlos a las necesidades del negocio.

Información principal

Descripción del producto	Cisco Catalyst 3560G-24TS - conmutador - 24 puertos
Tipo de dispositivo	Conmutador
Factor de forma	Externo - 1U
Dimensiones (Ancho x Profundidad x Altura)	44.5 cm x 37.8 cm x 4.4 cm
Peso	5.4 kg
Cantidad de puertos	24 x Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T
Velocidad de transferencia de datos	1 Gbps
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Ranuras vacías	4 x SFP (mini-GBIC)
Modo comunicación	Semidúplex, dúplex pleno
Características	Capacidad duplex, negociación automática, activable
Cumplimiento de normas	IEEE 802.3ab
Alimentación	CA 120/230 V (50/60 Hz)

Especificaciones ampliadas

General

Tipo de dispositivo	Conmutador
Tipo incluido	Externo - 1U
Anchura	44.5 cm
Profundidad	37.8 cm
Altura	4.4 cm
Peso	5.4 kg

Conexión de redes

Cantidad de puertos	24 x Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T
Velocidad de transferencia de datos	1 Gbps
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Tecnología de conectividad	Cableado
Modo comunicación	Semidúplex, dúplex pleno
Protocolo de conmutación	Ethernet

Indicadores de estado	Estado puerto, velocidad de transmisión del puerto, modo puerto duplex, alimentación
Características	Capacidad duplex, negociación automática, activable
Cumplimiento de normas	IEEE 802.3ab

Expansión / Conectividad

Total ranuras de expansión (libres)	4 (4) x SFP (mini-GBIC)
Interfaces	24 x red - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45 1 x gestión - consola - RJ-45

Diverso

Kit de montaje en bastidor	Incluido

Alimentación

Dispositivo de alimentación	Fuente de alimentación - interna
Voltaje necesario	CA 120/230 V (50/60 Hz)
Consumo eléctrico en funcionamiento	100 vatios
Características	Contector de sistema de alimentación redundante (RPS)

Software / Requisitos del sistema

Software incluido	Standard Image (SI) Software

Parámetros de entorno

Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	45 °C
Ámbito de humedad de funcionamiento	10 - 85%

Accesorios

Adaptadores de red	
GLC-LH-SM=	Cisco - Módulo de transceptor - SFP - Gigabit EN - 1000Base-LX, 1000Base-LH - 1300 nm
CWDM-SFP-1590=	Cisco CWDM SFP - Módulo de transceptor - SFP - Gigabit EN, 2Gb Fibre Channel - CWDM - 1590 nm
GLC-T=	Cisco - Módulo de transceptor - SFP - Gigabit EN - 1000Base-T
CWDM-SFP-1550=	Cisco CWDM SFP - Módulo de transceptor - SFP - Gigabit EN, 2Gb Fibre Channel - CWDM - 1550 nm
GLC-SX-MM=	Cisco - Módulo de transceptor - SFP - Gigabit EN - 1000Base-SX - 850 nm
CWDM-SFP-1490=	Cisco CWDM SFP - Módulo de transceptor - SFP - Gigabit EN, 2Gb Fibre Channel - CWDM - 1490 nm
CWDM-SFP-1510=	Cisco CWDM SFP - Módulo de transceptor - SFP - Gigabit EN, 2Gb Fibre Channel - CWDM - 1510 nm
CWDM-SFP-1470=	Cisco CWDM SFP - Módulo de transceptor - SFP - Gigabit EN, 2Gb Fibre Channel - CWDM - 1470 nm
Cables de red	
CAB-SFP-50CM=	Cisco - Cable de interconexión - SFP (M) - SFP (M) - 50 cm
Accesorios de red	
RCKMNT-REC-1RU=	Cisco - Kit de montaje rack - 1U
RCKMNT-REC-1RU	Cisco - Kit de montaje rack - 1U
RCKMNT-1RU=	Cisco - Kit de montaje rack

ANEXO C.
TIA/EIA – 568 A-B

Sistema de Cableado Estructurado

Written by Evelio Martinez

Antecedentes

En el pasado había dos especificaciones principales de terminación de cableado: Los cables de datos y por otro lado, los cables de voz.

En la actualidad, los sistemas de Cableado Estructurado (CE) soportan una gran cantidad de servicios y aplicaciones (voz, datos, video, texto, imágenes), tales como:

- Teléfonos, conmutadores
- TV, Audio estéreo, DVD, VCR
- Computadoras
- Modems, Máquinas de fax
- Home Theater
- Receptores de satélite
- Sistemas de seguridad
- Sistemas de Automatización
- Control de luces
- Enrutadores/*switches*/access points/

En 1985 muchas compañías de la industria de las telecomunicaciones estaban desconcertadas por la falta de estándares de cableado. Entonces la EIA (Electronics Industries Associations) se puso a desarrollar un estándar para este propósito. el primer borrador (draft) del estándar no fue liberado sino hasta julio de 1991, y se le fue dado el nombre de EIA/TIA-568. en 1994 el estándar fue renombrado a TIA/EIA 568A, el existente estándar de AT&T 258A fue incluido y referenciado como TIA/EIA-568B. Estos estándares de facto se hicieron populares y ampliamente usados, despues fueron adoptados por organismos internacionales como el ISO/IEC 11801:1995.

Qué es el Sistema de Cableado Estructurado
El sistema de cableado estructurado (SCE) es una serie de estándares definidos por la TIA/EIA que definen como *diseñar*, *construir* y *administrar* un sistema de cableado que es estructurado, es decir, que el sistema está diseñado en bloques que tienen características de desempeño muy específicas.

Un SCE se refiere a todo el cableado y componentes instalados en una red basados en un orden lógico y organizado.

Organizaciones de estándares de cableado

Hay muchas organizaciones involucradas en el cableado estructurado en el mundo. En Estados Unidos es la ANSI, TIA e EIA, Internacionalmente es la ISO (International Standards Organization). El propósito de las organizaciones de estándares es formular un conjunto de reglas comunes para todos en la industria, en el caso del cableado estructurado para própositos comerciales es proveer un conjunto estándar de reglas que permitan el soporte de múltiples marcas o fabricantes. Existen varias referencias en SCE alrededor del mundo, tales como:

- **EIA/TIA 568A/B** El primer estándar de cableado estructurado Publicado en EUA por la EIA/TIA en 1991

- **ISO/IEC 11801** Versión internacional del estándar 568

- **CENELEC EN 50173** Estándar de cableado estructurado británico

- **CSA T529** Estándar de cableado estructurado Canadiense

El estándar de cableado estructurado EIA/TIA 568 fue diseñado para:

- Un sistema de cableado genérico de telecomunicaciones para edificios comerciales
- Definir tipo de medio, topología, terminaciones y puntos de conexión y administración
- Soportar ambiente de múltiples vendedores y productos
- Dirección para diseño futuro de productos de telecomunicaciones para empresas comerciales
- La habilidad para planear e instalar cableado de telecomunicaciones para edificios comerciales sin previo conocimiento de los productos que se utilizaran en el cableado.

Quiza la principal función de un SCE es **prevenir**, **aislar**, **identificar** y **corregir** fallas en una red de área local.

Los 6 subsistemas del sistema de cableado estructurado

1. Entrada al edificio:

La entrada a las servicios del edificio es el punto en el cual el cableado externo hace interfaz con el cableado de la dorsal dentro del edificio. Este punto consiste en la entrada de los servicios de telecomunicaciones al edificio (acometidas), incluyendo el punto de entrada a través de la pared y hasta el cuarto o espacio de entrada. Los requerimientos de la inteface de red están definidos en el estándar TIA/EIA-569A

2. Cuarto de equipos

El cuarto de equipos es un espacio centralizado dentro del edificio donde se albergan los equipos de red (enrutadores, *switches*, mux, dtu), equipos de datos (PBXs,..), video, etc. Los aspectos de diseño del cuarto de equipos está especificado en el estándar TIA/EIA 569A.

3. Cableado de la dorsal (backbone)

El cableado de la dorsal permite la interconexión entre los gabinetes de telecomunicaciones, cuartos de telecomunicaciones y los servicios de la entrada. Consiste de cables de dorsalm cross-connects principales y secundarios, terminaciones mecánicas y regletas o *jumpers* usados conexión dorsal-a-dorsal. Esto incluye:

- » Conexión vertical entre pisos (risers)
- » Cables entre un cuarto de equipos y cable de entrada a los servicios del edificio.
- » Cables entre edificios.

Tipo de cables requeridos para la Dorsal

Tipo de Cable	Distancias máximas de la dorsal
100 ohm UTP (24 or 22 AWG)	800 metros (Voz)
150 ohm STP	90 metros (Datos)
Fibra Multimodo 62.5/125 µm	2,000 metros
fibra Monomodo 8.3/125 µm	3,000 metros

4. Gabinete o rack de Telecomunicaciones

El rack de telecomunicaciones es el area dentro de un edificio que alberga el equipo del sistema de cableado de telecomunicaciones. Este incluye las terminaciones mecánicas y/o

cross-conects para el sistema de cableado a la dorsal y horizontal.

5. Cableado horizontal

El sistema de cableado horizontal se extiende desde el área de trabajo de telecomunicationes al rack de telecomunicaciones y consiste de lo siguiente:

- » Cableado horizintal
- » Enchufe de telecomunicaciones
- » Terminaciones de cable (asignaciones de guías del conector modular RJ-45)
- » Conexiones de transición

Tres tipos de medios son reconocidos para el cableado horizontal, cada uno debe de tener una extensión máxima de 90 metros:

- » Cable UTP 100-ohm, 4-pares, (24 AWG solido)
- » Cable 150-ohm STP, 2-pares
- » Fibra óptica 62.5/125-µm, 2 fibras

6. Area de trabajo

Los componentes del área de trabajo se extienden desde el enchufe de telecomunicaciones a los dispositivos o estaciónes de trabajo.

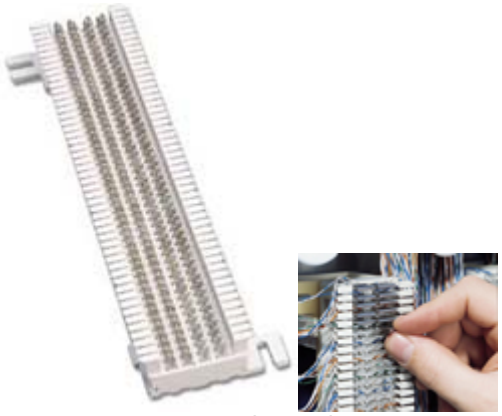
Los componentes del área de trabajo son los siguientes:

- » Dispositivos: computadoras, terminales, teléfonos, etc.
- » Cables de parcheo: cables modulares, cables adaptadores/conversores, jumpers de fibra, etc.
- » Adaptadores - deberán ser externos al enchufe de telecomununicaciones.

Varios tipos de enchufes (oulets) de pared para telecomunicaciones

Racks o gabinetes de telecomunicaciones

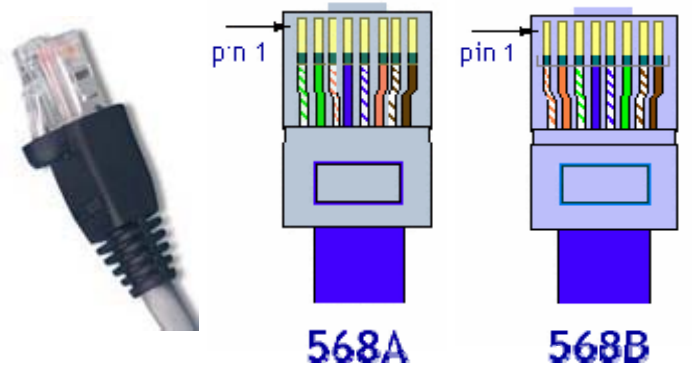
Paneles de parcheo (patch panel)

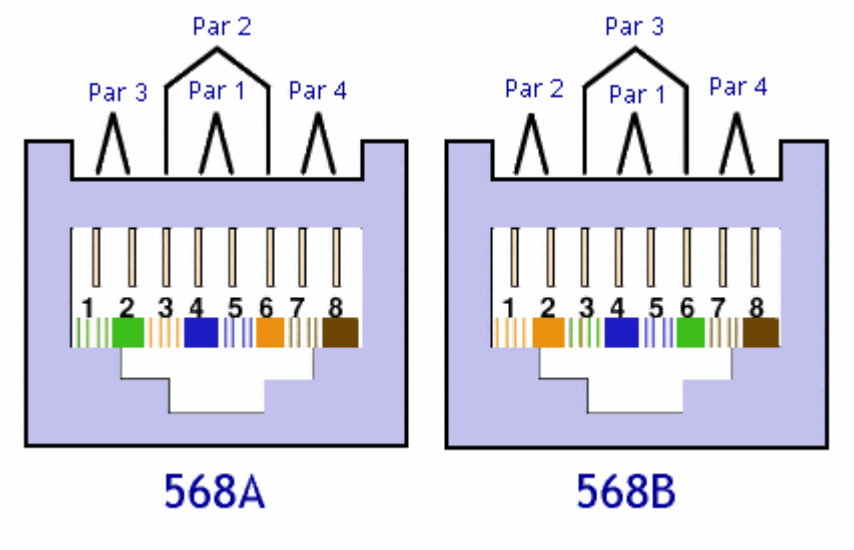


Tableros de conexión telefónica (s66)

Asignaciones del conector modular RJ-45 de 8 hilos, que forma parte del cableado horizontal.

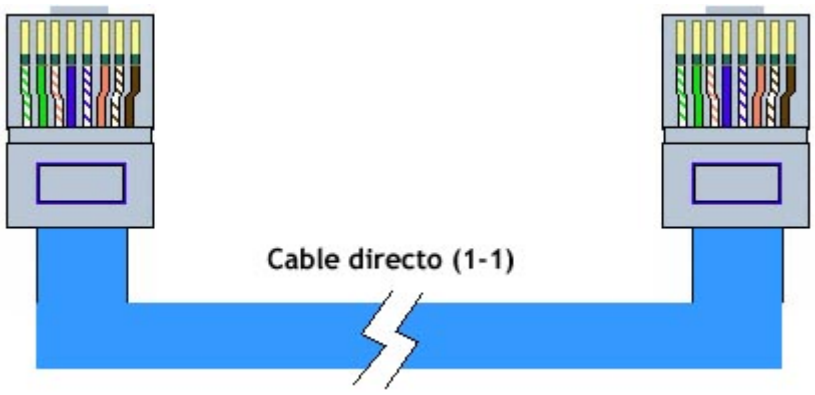
El conector RJ45 o RJ48 de 8 hilos/posiciones es el más empleado para aplicaciones de redes (El término RJ viene de *Registered Jack*). También existen Jacks, de 6 posiciones y de 4 posiciones (e.g. el jack telefónico de 4 hilos conocido como RJ11). Los conectores de 8 posiciones están numerados del 1 a 8, de izquierda a derecha, cuando el conector es visto desde la parte posterior al ganchito (la parte plana de los contactos), tal como se muestra en las figuras.





Como ya vimos, dos esquemas de asignación de pins están definidos por la EIA/TIA, el 568A y el 568B. Ambos esquemas son casi identicos, excepto que los pares 2 y 3, están al reves.

Cualquier configuración puede ser usada para ISDN (Integrated Services Digital Network) y aplicaciones de alta velocidad. Las Categorias de cables tranmisión 3,4, 5, 5e y 6 son sólo aplicables a este tipo de grupos de pares. Para aplicaciones de RED, (e.g. Ethernet 10/100BaseT, o Token Ring) solo son usados dos pares, los 2 pares restantes se utilizarian para otro tipo de aplicaciones, voz, por ejemplo.



¿Como leer un cable modular?

Alinear los dos extremos del conector, con los dos contactos hacia el frente y compare los colores de izquierda a derecha. Si los colores aparecen en el mismo orden en ambos conectores, entonces, el cable es "directo", o 1 a 1. Si los colores del segundo conector aparecen en sentido inverso al del primero, entonces, el cable es "cruzado".

Un **cable directo** sirve para conectar una computadora [tarjeta de red] a un Hub, o Una computadora a un *Switch*. Mientras que un **cable cruzado** sirve para conectar dos PCs entre sí; dos hubs o *switches* entre sí. Algunos hubs o *switches* pueden tener enchufes que cambien de directo a cruzado mediante un interruptor, otros tienen un enchufe especial para ese propósito marcado con "X".

¿Cómo hacer cables UTP de par trenzado?

Cómo vimos anteriormente existen 2 estándares para hacer cables UTP, el 568A y el 568B. La idea es que aprendamos a hacer cables usando estos 2 estándares, reiterando que la única diferencia son el orden de los colores. Al rato explicaremos porqué es necesario aprender los 2 estándares.

Qué material es necesario:
- 1 metro de cable par trenzado UTP categoría 5
- 3 conectores RJ45
- Pinzas de presión para par trenzado
- Probador de cables

Haciendo cables directos

Para hacer cables directos sólo hay que conectar ambos extremos de los cables siguiendo el mismo orden de colores en cada extremo.

Pin#	Función	568A	568B
1	Tx	BLANCO/VERDE	BLANCO/NARANJA
2	Tx	VERDE	NARANJA
3	Rx	BLANCO/NARANJA	BLANCO/VERDE
4	-	AZUL	AZUL
5	-	BLANCO/AZUL	BLANCO/AZUL
6	Rx	NARANJA	VERDE
7	-	BLANCO/CAFE	BLANCO/CAFE
8	-	CAFE	CAFE

Haciendo cables cruzados

Para hace cables cruzados (crossover), sólo hay que conectar en un extremo del conector RJ45 empleando el estándar 568A, y en el otro extremo del cable el estándar 568B. Asi de fácil.

PASOS para hacer un cable

1.- Cortar un trozo de cable
2.- Quitar el revestimiento.
3.- Separar los 4 pares de hilos.
4.- Destrenzar los hilos.
5.- Organizar los hilos según el código de color adecuado y aplanarlos.
6.- Mantener el orden de los colores y mantener los hilos aplanados, luego recorte los hilos de tal manera que la longitud 7.- máxima de los hilos no trenzados sea 1 o 2 cm.
7.- Insertar los hilos de forma ordenada en el conector RJ-45; asegúrese de que el revestimiento quede dentro del conector.
8.- Introduzca los hilos tan firmemente como sea posible para asegurarse de que los conductores se puedan ver cuando se mira el conector desde el extremo.
9.- Inspeccione el código de color y la ubicación de las envolturas para asegurarse de que sean los correctos.
10.- Inserte el conector firmemente en las pinzas y ciérrela totalmente a presión.
11.- Inspeccione ambos extremos de forma visual y mecánica.
12.- Utilice un prohador de cables para verificar la continuidad de c/u de los hilos del cable

ANEXO D.
RFC 1918

Network Working Group
Request for Comments: 1918
Obsoletes: 1627, 1597
BCP: 5
Categoría: Mejor Práctica Actual

Y. Rekhter
Cisco Systems
B. Moskowitz
Chrysler Corp.
D. Karrenberg
RIPE NCC
G. J. de Groot
RIPE NCC
E. Lear
Silicon Graphics, Inc.
Febrero 1996

Asignación de direcciones para Internet privadas

Status de este memorándum

Este documento especifica unas "Mejores Prácticas Actuales", Best Current Practices (BCP), para la comunidad Internet, y solicita su discusión y sugerencias para mejorarlas. La distribución de este memorándum es ilimitada.

1. Introducción

Para los propósitos de este documento, una empresa es una entidad que maneja de manera autónoma una red usando TCP/IP y en particular, que determina el plan de direccionamiento y las asignaciones de direcciones dentro de esa red.

Este documento describe la asignación de direcciones en las redes privadas. La asignación permite la completa conectividad de nivel de red entre todas las máquinas de la empresa así como entre todas las máquinas públicas de diferentes empresas. El coste de usar un espacio privado de direcciones de Internet es el coste potencial del esfuerzo de reasignar las direcciones de las máquinas y redes de públicos a privados.

2. Motivación

Con la proliferación mundial de la tecnología TCP/IP, incluso fuera de la propia Internet, un creciente número de empresas no conectadas usan esta tecnología y sus capacidades de direccionamiento únicamente para las comunicaciones internas, sin intención alguna de en algún momento conectarse directamente a otras empresas o a la propia Internet.

Internet ha crecido más allá de todas las previsiones. El continuo crecimiento exponencial continúa presentando nuevos retos. Uno de los retos es la constancia dentro de la comunidad de que el espacio de direcciones globalmente únicas se agotará. Un asunto distinto y bastante más acuciante es que la sobrecarga de encaminamiento crecerá más allá de las capacidades de los "Proveedores de Servicios de Internet", Internet Service Providers (ISP). Dentro de la comunidad existen iniciativas en curso para encontrar soluciones duraderas para ambos problemas. Mientras tanto es necesario reconsiderar los

procedimientos de asignación de direcciones, y su impacto en el sistema de encaminamiento de Internet.

Para contener el aumento en la sobrecarga de encaminamiento, un proveedor de Internet obtiene un bloque de espacio de direcciones de un registro de direcciones, y entonces asigna a sus clientes direcciones de ese bloque según las necesidades de cada cliente. El resultado de este proceso es que las rutas hacia muchos clientes pueden ser agrupadas, y aparecerán a los demás proveedores como una sola ruta [RFC1518], [RFC1519]. Para que esta agregación de rutas sea efectiva, los proveedores de Internet animarán a los clientes que se unan a su red a usar el bloque de direcciones del proveedor, y en consecuencia a renumerar sus máquinas. En el futuro, lo que ahora es una recomendación podría convertirse en una obligación.

Con el actual tamaño de Internet y su ritmo de crecimiento ya no es realista asumir que por el hecho de obtener una dirección IP globalmente única de un registro de Internet, la organización que consiga dicha dirección dispondrá de conectividad IP en todo Internet una vez dicha organización se conecte a Internet. Todo lo contrario, es bastante probable que cuando la organización se conecte a Internet para alcanzar conectividad IP global en Internet la organización tenga que cambiar las direcciones IP (renumerar) todas sus máquinas públicas (las máquinas que necesitan conectividad IP global en Internet), independientemente de si las direcciones inicialmente usadas por la organización eran globalmente únicas o no.

Ha sido típico asignar direcciones globalmente únicas a todas las máquinas que usan TCP/IP. Para prolongar la vida del espacio de direcciones IPv4, los registros de direcciones solicitan más justificaciones que nunca, haciendo más difícil que las organizaciones obtengan espacios de direcciones adicionales [RFC1466].

Se pueden dividir en tres categorías las máquinas que usan IP dentro de las empresas:

Categoría 1: máquinas que no necesitan acceder a máquinas en otras empresas, o Internet en general; las máquinas dentro de esta categoría pueden usar direcciones IP que sean únicas dentro de la empresa, pero que pueden no ser únicas entre empresas.

Categoría 2: máquinas que necesitan acceso a un conjunto reducido de servicios externos (por ejemplo, e-mail, FTP, news, login remoto) que pueden ser gestionados por pasarelas intermedias (por ejemplo, pasarelas de nivel de aplicación). Para muchas máquinas en esta categoría, un acceso sin restricciones al exterior (el proporcionado por la conectividad IP) puede ser innecesario e incluso no deseable por razones de seguridad y/o privacidad. Como en el caso de las máquinas en la primera categoría, tales máquinas pueden usar direcciones IP que sean únicas dentro de la empresa, pero que puedan ser ambiguas entre empresas distintas.

Categoría 3: máquinas que necesitan acceso de nivel de red hacia el exterior de la empresa (proporcionado mediante la conectividad IP); las máquinas en esta última categoría necesitan direcciones IP que sean

globalmente únicas.

Nos referiremos a las máquinas en la primera y segunda categorías como "privadas". Nos referiremos a las máquinas en la tercera categoría como "públicas".

Muchas aplicaciones necesitan conectividad sólo dentro de una empresa y no necesitan conectividad externa (fuera de la empresa) para la mayoría de las máquinas internas. En frecuente que en las grandes empresas sea sencillo identificar un considerable número de máquinas usando TCP/IP que no necesitan conectividad de nivel de red fuera de la empresa.

Algunos ejemplos donde la conectividad externa podría no ser necesaria son:

- Un gran aeropuerto que tiene sus pantallas de llegadas y salidas direccionables individualmente mediante TCP/IP. Es muy improbable que estas pantallas necesiten ser directamente accesibles desde otras redes.

- Grandes organizaciones como bancos y cadenas de pequeños comercios que estén cambiando a TCP/IP para sus comunicaciones internas. El elevado número de puestos locales tales como cajas registradoras, dispensadores de efectivo, y equipamiento en otros puestos raramente necesitan disponer de tal conectividad.

- Por razones de seguridad, muchas empresas usan pasarelas de nivel de aplicación para conectar sus redes internas a Internet. A menudo las redes internas no tienen acceso directo a Internet, y sólo una o más pasarelas son visibles desde Internet. En este caso, la red interna puede usar números de red IP no únicos.

- Las interfaces de los encaminadores en una red interna a menudo no necesitan ser directamente accesibles desde fuera de la empresa.

3. Espacio de direcciones privado

La "Autoridad de Números Asignados en Internet", Internet Assigned Numbers Authority (IANA), ha reservado los tres siguientes bloques de direcciones IP para el uso en internets privadas:

```
10.0.0.0        -   10.255.255.255  (prefijo 10/8)
172.16.0.0      -   172.31.255.255  (prefijo 172.16/12)
192.168.0.0     -   192.168.255.255 (prefijo 192.168/16)
```

Nos referiremos al primer bloque como "bloque de 24 bits", al segundo como "bloque de 20 bits" y al tercero como "bloque de 16 bits". Dese cuenta que (en la notación anterior a CIDR) el primer bloque no es más que un único número de red de clase A, mientras que el segundo bloque es un conjunto de 16 números de red de clase B contiguos, y el tercer bloque es un conjunto de 256 números de red de clase C contiguos.

Una empresa que decida usar direcciones IP del espacio de direcciones definido en este documento puede hacerlo sin tener que coordinarse con la IANA o con un registro de Internet. De esta manera el espacio de direcciones puede ser usado por muchas empresas. Las direcciones de este espacio de direcciones privado sólo serán únicas dentro de la

empresa, o el conjunto de empresas que elijan colaborar sobre este espacio para que puedan comunicarse con las demás en su propia internet privada.

Como antes, cualquier empresa que necesite espacio de direcciones globalmente único necesita obtener tales direcciones de un registro de Internet. Una empresa que solicite direcciones IP para su conectividad externa nunca recibirá direcciones de los bloques definidos arriba.

Para usar el espacio de direcciones privado, una empresa necesita determinar qué máquinas no necesitan disponer de conectividad de nivel de red hacia el exterior de la empresa en un futuro previsible y así poder clasificarlas como privadas. Tales máquinas usarán el espacio de direcciones privado definido anteriormente. Las máquinas privadas pueden comunicarse con el resto de máquinas de la empresa, tanto públicas como privadas. Sin embargo, no pueden tener conectividad IP a ninguna máquina fuera de la empresa. Aunque no dispongan de conectividad IP externa (fuera de la empresa), las máquinas privadas aún pueden tener acceso a servicios externos mediante el uso de pasarelas (por ejemplo, pasarelas de nivel de aplicación).

El resto de máquinas serán públicas y usarán espacio de direcciones globalmente únicas asignadas por un registro de Internet. Las máquinas públicas pueden comunicarse con otras máquinas dentro de la empresa, tanto públicas como privadas, y pueden tener conectividad IP con máquinas públicas fuera de la empresa. Las máquinas públicas no tienen conectividad con las máquinas privadas de otras empresas.

Cambiar una máquina de privada a pública o viceversa implica un cambio de dirección IP, cambios en las entradas DNS correspondientes, y cambios en los ficheros de configuración de otras máquinas que referencien a la máquina por su dirección IP.

Puesto que las direcciones privadas no tienen significado global, la información de encaminamiento acerca de las redes privadas no se propagará en los enlaces entre empresas, y los paquetes con direcciones origen o destino privadas no deberían ser reenviados por dichos enlaces. Se supone que los encaminadores en las redes que no usen espacio de direcciones privados, especialmente aquéllos situados en los proveedores de servicios de Internet, estarán configurados para rechazar (filtrar) la información de encaminamiento acerca de redes privadas. Si uno de estos encaminadores recibe tal información, el rechazo no será tratado como un error en el protocolo de encaminamiento.

Las referencias indirectas a tales direcciones deberán quedar limitadas a los límites de la empresa. Ejemplos significativos de estas referencias son los "Registros de Recursos DNS", DNS Resource Records, y otra información importante acerca de las direcciones privadas internas. En particular, los proveedores de servicios de Internet deberían tomar medidas para evitar dichas fugas de información.

4. Ventajas y desventajas de usar espacio de direcciones privado

La ventaja obvia de usar espacio de direccionamiento privado de manera global es conservar el espacio de direcciones globalmente únicas no usando estas direcciones donde no sea necesaria esta unicidad.

Las propias empresas también obtendrán ciertas ventajas por el uso del espacio de direccionamiento privado: ganan gran flexibilidad en el diseño de la red al tener más espacio de direcciones a su disposición del que dispondrían obteniendo direcciones globalmente únicas. Esto permite esquemas de direccionamiento operacional y administrativamente provechosos, así como una sencilla escalabilidad.

Por diversas razones, en Internet se han dados casos en los que una empresa que no está conectada a Internet ha usado direcciones IP para sus máquinas sin haberlas solicitado previamente a la IANA. En algunos casos este espacio de direcciones ya ha sido asignado a otras empresas. Si posteriormente tal empresa se conecta a Internet, esto podría potencialmente crear problemas muy graves, puesto que el encaminamiento IP no puede funcionar correctamente en presencia de direccionamiento ambiguo. Aunque en principio los proveedores de servicios de Internet deberían protegerse de tales errores mediante el uso de filtros de rutas, en la práctica no siempre sucede así. El uso del espacio de direcciones privado proporciona una elección segura para tales empresas, evitando conflictos cuando sea necesaria la conectividad externa.

Uno de los principales inconvenientes del uso de direcciones privadas es que puede reducir la flexibilidad de la empresa para salir a Internet. Cuando se compromete a usar direcciones privadas, se está comprometiendo a renumerar parte o toda la empresa, si se decidiera a proporcionar conectividad IP entre esa parte (o toda la empresa) e Internet. A menudo el coste de renumerar puede medirse contando el número de máquinas que deben pasar de privado a público. Sin embargo, como se discutió previamente, incluso si una red usa direcciones globalmente únicas, aún puede ser necesario tener que renumerar para lograr conectividad IP hacia todo Internet.

Otro perjuicio de usar espacio de direcciones privado es que puede obligar a renumerar cuando se unan varias redes privadas en una única red física privada. Si revisamos los ejemplos enumerados en la sección 2, nos daremos cuenta que las compañías tienden a unirse. Si previamente a la unión dichas compañías mantuviesen sus propias redes usando direccionamiento privado, entonces si después de la unión estas redes se combinasen en una sola, algunas direcciones dentro de la red combinada podrían no ser únicas. Como resultado, las máquinas con dichas direcciones deberían ser renumeradas.

El coste de la renumeración también puede ser reducido por el desarrollo y despliegue de herramientas que faciliten la renumeración (por ejemplo, "Protocolo de Configuración Dinámica de Máquinas", Dynamic Host Configuration Protocol (DHCP)). Cuando se esté planteando si usar direcciones privadas, recomendamos consultar a los fabricantes de hardware y software sobre la disponibilidad de dichas herramientas. Un esfuerzo separado del IETF (PIER Working Group) está intentando documentar completamente los requisitos y procedimientos para la renumeración.

5. Consideraciones operacionales

Una estrategia posible es diseñar primero la parte privada de la red y usar el espacio de direcciones privado para todos los enlaces internos. Entonces, planificar las subredes públicas en las localizaciones necesarias y diseñar la conectividad externa.

Este diseño no tiene porqué ser indefinidamente fijo. Si

posteriormente un grupo de una o más máquinas necesita cambiar su status (de privado a público, o viceversa), esto se puede hacer renumerando sólo las máquinas involucradas, y cambiando la conectividad física en caso necesario. En localizaciones donde dichos cambios sean previsibles (salas de ordenadores, etc.), es aconsejable configurar medios físicos separados para las subredes pública y privada, y así facilitar tales cambios. Para evitar intervenciones de importancia en la red, es aconsejable agrupar en sus propias subredes máquinas con similares necesidades de conectividad.

Si se puede diseñar un adecuado esquema de división en subredes que esté soportado por el equipamiento implicado, es aconsejable usar el espacio privado de direcciones del bloque de 24 bits (red de clase A) y diseñar un plan de direccionamiento con un buen camino de crecimiento. Si el hacer las subredes es problemático se puede usar el espacio de direcciones del bloque de 16 bits (redes de clase C) o del bloque de 20 bits (redes de clase B).

Se podría estar tentado de tener tanto direcciones públicas como privadas en el mismo medio físico. Aunque es posible, existen riesgos en tales diseños (dese cuenta que los riesgos no tienen nada que ver con el uso de direcciones privadas, sino que son debidos a la presencia de múltiples subredes IP en una misma subred física de datos). Aconsejamos prudencia cuando se trabaje en estos supuestos.

Se recomienda encarecidamente que los encaminadores que conectan las empresas a las redes externas se configuren con los filtros de paquetes y rutas adecuados en ambos extremos del enlace para evitar fugas de paquetes e información de encaminamiento. Una empresa también debería aislar a cualquier red privada de la información de encaminamiento entrante para protegerse a sí misma de situaciones de encaminamiento ambiguas que pueden presentarse si las rutas hacia el espacio de direcciones privadas apunta hacia fuera de la empresa.

Es posible que ambos sitios, que coordinan sus respectivos espacios de direcciones privadas, se comuniquen con el otro sobre una red pública. Para hacer esto deben usar algún método de encapsulamiento en sus fronteras con la red pública, manteniendo privadas sus direcciones privadas.

Si dos (o más) organizaciones implementan la asignación de direcciones especificada en este documento y más tarde desean establecer conectividad IP con las demás, existe el riesgo de que la unicidad en las direcciones pueda violarse. Para minimizar el riesgo es altamente recomendable que una organización que use direcciones IP privadas elija aleatoriamente de la lista de direcciones privadas, cuando asigne sub-bloques en su asignación interna.

Si una empresa usa espacio de direcciones privado, o una mezcla de espacios de direcciones privado y públicos, entonces los clientes DNS externos a la empresa no deberían ver direcciones en el espacio de direcciones privado usado por la empresa, puesto que estas direcciones serían ambiguas. Una manera de asegurarse de esto es disponer de dos servidores de nombres autorizados para cada zona DNS que contengan las direcciones tanto públicas como privadas de las máquinas. Un servidor sería visible desde el espacio de direcciones público y contendría sólo el subconjunto de direcciones de la empresa alcanzables mediante direcciones públicas. El otro servidor sería alcanzable sólo desde la red privada y contendría el conjunto completo de datos, incluyendo las direcciones privadas y cualesquiera otras direcciones públicas alcanzables desde la red privada. Para

asegurar la consistencia, ambos servidores deberían configurarse a partir de los mismos datos, de los cuales la zona públicamente visible sólo contiene una versión filtrada. Hay cierto grado de complejidad adicional asociada con la provisión de estas capacidades.

6. Consideraciones de seguridad

Las consideraciones de seguridad no se tratan en este memorándum.

7. Conclusión

Con el esquema descrito muchas grandes empresas sólo necesitarán un bloque relativamente pequeño de direcciones del espacio de direcciones IP globalmente únicas. Todo Internet se beneficia del ahorro del espacio de direcciones globalmente únicas que tendrá como efecto el aumento en la vida del espacio de direcciones IP. Las empresas se benefician de la flexibilidad adicional proporcionada por un espacio de direcciones privadas relativamente grande. Sin embargo, el uso de direccionamiento privado requiere que una organización renumere parte o la totalidad de su red empresarial, puesto que sus necesidades de conectividad cambian con el tiempo.

8. Reconocimientos

Nos gustaría agradecer a Tony Bates (MCI), Jordan Becker (ANS), Hans-Werner Braun (SDSC), Ross Callon (BayNetworks), John Curran (BBN Planet), Vince Fuller (BBN Planet), Tony Li (cisco Systems), Anne Lord (RIPE NCC), Milo Medin (NSI), Marten Terpstra (BayNetworks), Geza Turchanyi (RIPE NCC), Christophe Wolfhugel (Pasteur Institute), Andy Linton (connect.com.au), Brian Carpenter (CERN), Randy Bush (PSG), Erik Fair (Apple Computer), Dave Crocker (Brandenburg Consulting), Tom Kessler (SGI), Dave Piscitello (Core Competence), Matt Crawford (FNAL), Michael Patton (BBN), y a Paul Vixie (Internet Software Consortium) su revisión y comentarios constructivos acerca del documento.

9. Referencias

[1] [RFC1466] Gerich, E., "Guidelines for Management of IP Address Space", RFC 1466, Merit Network, Inc., Mayo 1993.

[2] [RFC1518] Rekhter, Y., and T. Li, "An Architecture for IP Address Allocation with CIDR", RFC 1518, Septiembre 1993.

[3] [RFC1519] Fuller, V., Li, T., Yu, J., and K. Varadhan, "Class less Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy", RFC 1519, Septiembre 1993.

10. Direcciones de los autores

Yakov Rekhter
Cisco systems
170 West Tasman Drive
San Jose, CA, USA
Phone: +1 914 528 0090
Fax: +1 408 526-4952
EMail: yakov@cisco.com

Robert G Moskowitz

Chrysler Corporation
CIMS: 424-73-00
25999 Lawrence Ave
Center Line, MI 48015
Phone: +1 810 758 8212
Fax: +1 810 758 8173
EMail: rgm3@is.chrysler.com

Daniel Karrenberg
RIPE Network Coordination Centre
Kruislaan 409
1098 SJ Amsterdam, the Netherlands
Phone: +31 20 592 5065
Fax: +31 20 592 5090
EMail: Daniel.Karrenberg@ripe.net

Geert Jan de Groot
RIPE Network Coordination Centre
Kruislaan 409
1098 SJ Amsterdam, the Netherlands
Phone: +31 20 592 5065
Fax: +31 20 592 5090
EMail: GeertJan.deGroot@ripe.net

Eliot Lear
Mail Stop 15-730
Silicon Graphics, Inc.
2011 N. Shoreline Blvd.
Mountain View, CA 94043-1389
Phone: +1 415 960 1980
Fax: +1 415 961 9584
EMail: lear@sgi.com

Traducción al castellano:

José Luis Domingo López
c/ Cruz del Sur 22
28007 Madrid - España

EMail: jdomingo@internautas.org