ANÁLISIS, DISEÑO Y OPTIMIZACIÓN DE UNA RED LOCAL CON INTERVLANS TRONCALIZADAS Y SEGURIDAD DE ACCESO MEDIANTE LA APLICACIÓN DE ACLS.

María Auxiliadora Desiderio Rodrigo[1], Pedro José Solís Sánchez[2], Ivonne Martín Moreno[3].

[1]Ingeniero Eléctrico en Telecomunicaciones 2006.
[2]Ingeniero Eléctrico en Telecomunicaciones 2006.
[3]Director de Tesis, Ingeniera Electrónica, Escuela Superior Politécnica del Litoral, 1991, Postgrado MAE ESPAE 1994, Profesora de la ESPOL desde 2002.

RESUMEN

En esta tesis diseñamos una red local con 3 VLANS, las cuales se comunican entre ellas de manera troncalizada, para este propósito empleamos un router que permite la comunicación entre ellas. Sobre nuestro diseño implementamos los 4 principales protocolos de enrutamiento que existen en la actualidad que son: RIP V1, RIP V2, IGRP, y, EIGRP, siendo estos dos últimos protocolos propietarios de la marca CISCO.

Realizamos pruebas de conectividad entre los distintos dispositivos que conformaron nuestra red, aplicando cada uno de los protocolos de enrutamiento detallados en este resumen, escogimos el mejor en base a la escalabilidad y convergencia, sobre la configuración de los routers con el protocolo seleccionado se aplicaron ACLS a las interfases tanto físicas como virtuales de los routers, con lo cual comprobamos el correcto funcionamiento de las ACLS.

También se efectuaron pruebas de redundancia aplicando Etherchannel, tecnología propietaria de CISCO, se simularon caídas de enlace, verificando de esta manera la continuidad de la conectividad de nuestra red.

SUMMARY

In this thesis we design a LAN with 3 VLANS, VLANS communicate each other in a Trunking way, and for this method we use a router that allows a communication InterVLAN. Over our design we improve the main four routing protocols that exist in this moment, they are: RIP V1, RIP V2, IGRP, EIGRP, the two last protocols are from CISCO.

We made connectivity probes between the different devices that form part of our Network, applying each one of the routing protocols detail in this resume, we choose the best due two characteristics: scalability and convergence, over the configuration in routers with the best routing protocol we apply ACLS to virtual and physic interfaces, verifying the correct function of ACLS.

We also make redundancy's probes applying ETHERCHANNEL, technology owner of CISCO, we simulate drops of links, probing that connectivity continues working in our design.

INTRODUCCIÓN

Las medianas a grandes empresas presentan grandes necesidades de comunicación como: tener subredes privadas con seguridad de acceso en ciertas de ellas por la información confidencial que manejan y mantener conectividad entre ellas, una subred que maneje solo los servidores para optimización en la conectividad y el manejo de aplicaciones, subredes que manejen los dispositivos pasivos de la compañía como: impresoras y faxes para la optimización de recursos, una subred para video conferencia y/o telefonía IP. Estas necesidades y otras adicionales hacen que una empresa decida en recurrir a gastos adicionales de equipos de conmutación como son los switches, uno por cada subred. Nuestra solución es la implementación de VLANS, una

VLAN por cada subred privada, para seguridad, control y gestión de todo tráfico que dentro de la red se maneje, esta solución nos va a permitir tener dominios de broadcast independientes dentro de un mismo switch que debe de ser bien robusto, ahorrando de esta manera la adquisión de un switch por cada VLAN, y manejando de una manera más inteligente la información que por las subredes va a pasar, es como tener switches virtuales(lógicos) dentro de un switch Físico.

Los dispositivos dentro de una misma VLAN se podrán comunicar entre sí, cuando necesitemos la comunicación entre las diferentes VLANS creadas, vamos a necesitar un dispositivo de capa de red como lo es el router, normalmente se necesitará un puerto en el router para cada VLAN implementada, por ende se deberá adquirir módulos ethernet adicionales y el uso de un puerto en el switch para cada VLAN. Esta solución no es la más óptima, para este propósito presentamos la conectividad entre VLANS de manera troncalizada, esto nos va a permitir que por un mismo puerto del switch y por un mismo puerto ethernet del router viajen la información de todas las VLANS que se necesiten compartir entre sí ahorrando puertos innecesarios dentro del switch y el gasto adicional de tarjetas ethernet en el router, esto permite un mayor control del tráfico broadcast que tanto daño le hace a la red sino se lo sabe gestionar de manera inteligente. Para esta solución se crean subinterfases en el router, cada subinterfase en el router va a manejar una VLAN, una subinterfase es una interfase virtual (lógica) que se crea a partir de una interfase física, en otras palabras por un mismo cable que está conectado de un extremo en el router y en el otro extremo en el switch, gracias a las subinterfases creadas en el router y al protocolo de comunicación Trunking InterVLAN el 802.1Q vamos a tener viajando a los paquetes de información de cualquier tipo que quieran pasar de una VLAN a otra.

CONTENIDO

CAPITULO 1
DISEÑO Y CONFIGURACION DE LA RED.

En este capítulo detallaremos el procedimiento para asignar las direcciones IP a los usuarios de nuestra red, evitando el desperdicio de las mismas, se aplicará el procedimiento de Subnetting y VLSM para crear las subredes necesarias y tener subredes adicionales para la escalabilidad de la red, en otras palabras tendremos subredes adicionales para así manejar correctamente el crecimiento de la red a futuro, además se tomará una dirección IP de red privada de clase B, porque nos permite tener muchos más usuarios por subred que una clase C, se analizará el direccionamiento de los equipos de Networking que conforman la red, y por último se configurará los equipos para la conectividad Trunking.

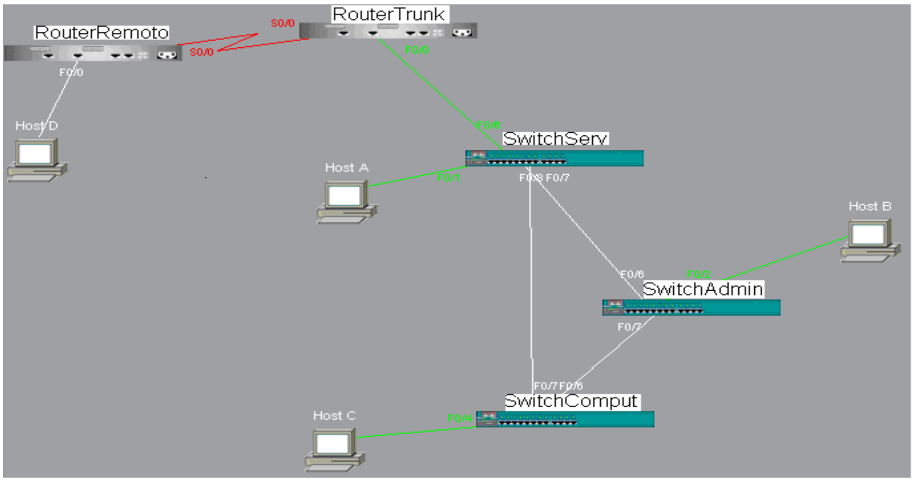

Figura 1 Red armada para las pruebas.

Para nuestras pruebas armamos la red mostrada en la figura **1**, en la cual vamos a probar la conectividad de los dispositivos con 4 protocolos de enrutamiento: **RIP V1**, **RIP V2**, **IGRP**, e **EIGRP**, y el protocolo **802.1q** para el enlace trunking.

Hemos tomado la red **172.16.0.0** y nuestra máscara será la **255.255.254.0** en las VLANS, recordando que ésta es una red privada de clase B cuya máscara por defecto es **255.255.0.0**, en otras palabras estamos realizando "Subnetting".

Hemos querido diseñar subredes con **510** hosts válidos para asegurar una escalabilidad dentro de las VLANS, esto significa tener direcciones de red disponibles para asignar a futuros usuarios, para este propósito hemos tomado 9 bits para cubrir los 510 hosts, en el método de subnetting mediante la formula: 2 ^ n – 2, donde n es el numero de bits prestados, para la parte de hosts n sería 9, se resta 2 en la fórmula debido a que no se toman dos direcciones dentro del rango, las cuales son: la primera que es la dirección de red de la subred y la última que es la dirección de broadcast.

Como dentro de una máscara por defecto en clase B tenemos 16 bits disponibles para realizar subnetting los cuales son los dos últimos octetos, y ya hemos tomado 9, entonces los bits restantes que son 7, los utilizamos para determinar la cantidad de subredes posibles gracias a la misma fórmula con que obtuvimos el número de usuarios: 2 ^ n – 2, ahora n es 7, esto nos indica que tenemos 126 subredes con 510 hosts disponibles cada una de ellas, así mismo la primera subred no se la toma en cuenta ni la última.

A continuación detallamos en la tabla cada subred a utilizar en las pruebas con su rango respectivo de direcciones IP útiles, no se presentan todas las subredes posibles.

número de subred	dirección de subred	rango de direcciones IP disponibles	dirección de broadcast	hosts	hosts útiles
1	172.16.0.0	172.16.0.1------172.16.1.254	172.16.1.255	512	510
2	172.16.2.0	172.16.2.1------172.16.3.254	172.16.3.255	512	510
3	172.16.4.0	172.16.4.1------172.16.5.254	172.16.5.255	512	510
4	172.16.6.0	172.16.6.1------172.16.7.254	172.16.7.255	512	510
5	172.16.8.0	172.16.8.1------172.16.9.254	172.16.9.255	512	510
6	172.16.10.0	172.16.10.1----172.16.11.254	172.16.11.255	512	510

Tabla I Direcciones IP de las subredes implementadas.

Hemos tomado la subred **172.16.2.0 /23** para asignarle a la **VLAN 1.**
Hemos tomado la subred **172.16.4.0 /23** para asignarle a la **VLAN 2**.
Hemos tomado la subred **172.16.6.0 /23** para asignarle a la **VLAN 3.**

El **/23** significa que las subredes tienen mascara **255.255.254.0**, esto significa que cada subred tiene la capacidad de **510** usuarios, como anteriormente ya lo explicamos.

El RouterTrunk es el que va a manejar la conectividad trunking entre las VLANS, permitiendo que los usuarios de distintas VLANS se comuniquen entre sí, a la vez el RouterTrunk gracias a un enlace serial con el RouterRemoto permite conectar a los usuarios de las distintas VLANS con una subred externa, a la cual le hemos asignado la dirección IP **172.16.8.0 /23** ,simulando con esto una conexión WAN.

Según el estándar **RFC 1918**, dentro de una red privada se pueden asignar direcciones IP desde la clase A a la clase C siendo los rangos, los siguientes:

- **Clase A: 10.0.0.0---10.255.255.255**
- **Clase B: 172.16.0.0---172.31.255.255**
- **Clase C: 192.168.0.0---192.168.255.255**

Cada switch dentro de una red se le debe asignar dirección IP para poder ser monitoreado vía telnet y para que funcione correctamente, por defecto antes de proceder con la creación de vlans, todos los puertos ethernet de un switch pertenecen a una sola vlan, la vlan 1 o también llamada a la vlan administrativa, esto quiere decir que todos los puertos del switch pertenecen al mismo dominio broadcast.
Las direcciones IP para cada switch fueron tomadas de la **VLAN 1** y son las siguientes:

- Dirección IP del SwitchServ: **172.16.2.2 / 23**

- Dirección IP del SwitchAdmin: **172.16.2.3 / 23**

- Dirección IP del SwitchComput: **172.16.2.4 / 23**

Además al switch se le debe de asignar una dirección por defecto, como los Switches están conectados en cascada deben de tener la misma dirección por defecto, la cual es: **172.16.2.1**, que es la dirección IP de la primera subinterfaz del puerto fastethernet 0/0 del RouterTrunk.
Los puertos 2 y 3 en cada switch fueron asignados para la VLAN 2 es decir la VLAN de alumnos. Los puertos 4 y 5 en cada switch fueron asignados para la VLAN 3 es decir la VLAN de profesores.
La verificación de la correcta configuración de los puertos asignados a las VLANS en cada switch, la podemos observar con ***show vlans*** dentro del modo privilegiado, vía consola o Telnet en cada switch.
Los puertos 6,7 y 8 en el SwitchServ fueron asignados para la comunicación Trunking. Los puertos 6 y 7 tanto en el SwitchAdmin como en el SwitchComput fueron asignados para la comunicación trunking.
La verificación de la correcta configuración de los puertos que pertenecen a la conectividad Trunking en cada switch la podemos observar con ***show Start*** dentro del modo privilegiado, vía consola o vía Telnet en cada switch.
un router puede manejar hasta más de 255 VLANS, esto depende del modelo del router, estas subinterfases son Interfases lógicas, al igual que las 3 VLANS creadas en el switch, cada subinterfase debe detener una dirección IP y una máscara de subred, esta dirección IP debe de pertenecer a la VLAN a la cual enruta . A continuación se detallan las direcciones IP que se asignaron a las subinterfases:

- Subinterfase 1 o interfase 0/0.1: **172.16.2.1/23**

- Subinterfase 2 o interfase 0/0.2: **172.16.4.1/23**

- Subinterfase 3 o interfase 0/0.3: **172.16.6.1/23**

Capitulo 2
PRUEBAS DE DESEMPEÑO DE LA RED.

En este capítulo se van a realizar pruebas de conectividad sobre la red mostrada en la figura **2** con los protocolos **RIP V1**, **IGRP**, **RIP V2** y **EIGRP**. Los equipos de la red se deben de conectar siguiendo el correcto cableado estructurado como se indica en normas como las: NORMA TIA/EIA 569-A, ANSI/TIA/EIA-568-A, TIA/EIA 568-B.2**.**
Con las conclusiones que se saque de las pruebas con cada uno de los protocolos, se va a escoger el más idóneo, el que nos permita tener una red más segura; Sobre ese protocolo se va a implementar las ACLS en las interfases de los routers.

Todas las pruebas se realizaron en equipos marca **CISCO**.

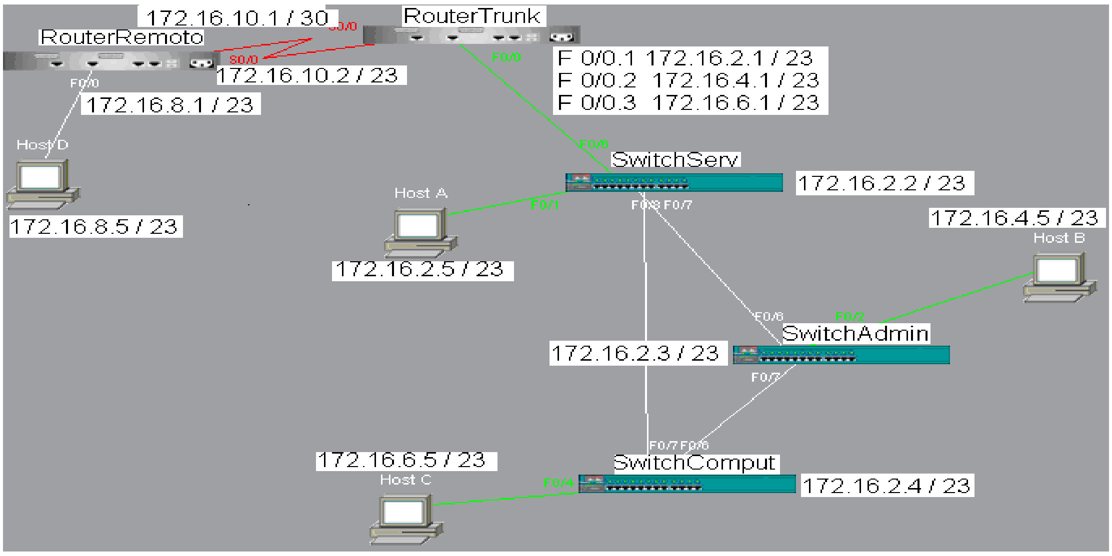

Figura 2 Red con direcciones IP respectivas.

Las pruebas que se realizaron se detallan a continuación:

1. Ping desde usuario de una VLAN a usuario de la misma VLAN.
2. Ping desde usuario de una VLAN a usuario de otra VLAN.
3. Ping desde usuario de una VLAN a los routers de la red.
4. Ping desde usuario de una VLAN a red remota.
5. Ping desde consola de cada switch a distintos puntos de la red.
6. Ping desde consola de los routers a distintos puntos de la red.
7. Ping desde red remota a usuarios de las distintas VLAN.
8. Telnet desde usuarios de las distintas VLAN hacia los routers.
9. Telnet desde usuario de red remota hacia routers de la red.

Llegando a los siguientes resúmenes:

Resumen de pruebas con RIP V1.

- Es un protocolo diseñado para redes pequeñas y no tan complejas.
- Es un protocolo que no soporta VLSM.
- Si un interfaz tiene máscara distinta al resto de redes, las actualizaciones no son enviadas por ese interfaz.
- Tener en cuenta la versión del protocolo RIP tanto de envío como de recepción de paquetes.
- Envía actualizaciones broadcast a 255.255.25.255.

Resumen de pruebas con IGRP.

- No propaga rutas con distintas máscaras de subred.
- No soporta VLSM.
- Es compatible con el protocolo EIGRP.
- Las métricas por defecto son: ancho de banda y retardo, aunque no se las toman en cuenta, la carga y la confiabilidad son métricas de IGRP.
- Se maneja por sistemas autónomos.
- Las actualizaciones las envía mediante broadcast (255.255.255.255)

Resumen de pruebas con RIP V2

- Es un protocolo que propaga rutas con distintas máscaras de subred.
- Soporta VLSM.
- Verificar si tanto en el envío como en la recepción esta correcta la versión del protocolo.
- Tiene las mismas características que RIP V1.
- Es la versión mejorada de RIP V1.
- Envía las actualizaciones a una dirección multicast (224.0.0.9).

Resumen de pruebas con EIGRP

- Es el protocolo más completo de todos los analizados en esta tesis.
- Es un protocolo que mantiene 3 tablas para una convergencia automática, ante cualquier cambio topológico.
- Es un protocolo sin clase el cual soporta VLSM y CIDR, por lo tanto se propagan todas las rutas conocidas por más máscaras variables que estén presentes en la red.
- Las actualizaciones se realizan ante un cambio topológico y solo se propagan los cambios.
- La comunicación entre routers se efectúa mediante el paquete HELLO que es un paquete sin datos así no satura el ancho de banda del enlace, y éste es enviado por defecto cada 5 segundos.
- Las actualizaciones son enviadas a una dirección multicast (224.0.0.10).

Resultados totales de las pruebas.

- Los protocolos de estado de enlace como EIGRP permiten una convergencia más rápida de los equipos ante un cambio topológico inesperado.
- Los protocolos sin clase permiten tener máscaras de subred variables dentro de una red, permitiendo así el ahorro de direcciones IP.
- Todo el conjunto de métricas que maneja EIGRP (ancho de banda, retardo, carga, confiabilidad), hacen de EIGRP el protocolo más confiable y seguro de todos.
- Gracias a las 3 tablas que maneja EIGRP (tabla vecino, tabla topología y tabla de enrutamiento), permite tener un conocimiento total de toda la red y tener presente rutas de respaldo, que se activan de manera automática ante algún cambio topológico.
- Los 5 tipos de paquetes que maneja EIGRP y su algoritmo de enrutamiento DUAL permiten mantener las rutas de menor costo hacia todos los puntos de la red y una comunicación constante entre equipos para actuar de manera inteligente y rápida ante la falla de algún enlace.

Hay muchas maneras de proteger la información y restringir el acceso de personas no autorizadas a una red, en esta tesis nos enfocamos a la implementación de Listas de Control de Acceso (ACLS). Se puede implementar ACLS tanto a las interfases físicas del router que son las que permiten la conectividad de los dispositivos de la red como a las interfases virtuales que permiten la configuración del router de manera externa. La primera nos permite la restricción al acceso de personas ajenas a la organización que puedan alterar información que la red maneja, y la segunda nos permite tener seguridad en que alguien no autorizado haga cambios en la configuración de los equipos activos (routers, switches) que afecten el funcionamiento de la red.

Además si tenemos varios switches conectados en cascada los mismos puertos que se asignan a una VLAN deben asignarse en todos los switches. Al configurarse los switches con Etherchannel, nos permite tener un enlace redundante entre switches, si es que ocurre una falla en el enlace principal, el enlace secundario permita una continuidad en la conectividad de la red. Además con etherchannel podemos duplicar el ancho de banda de transmisión porque a los dos cables se los considera uno solo, se los toma como un grupo en el momento de la configuración (ver figura 3).

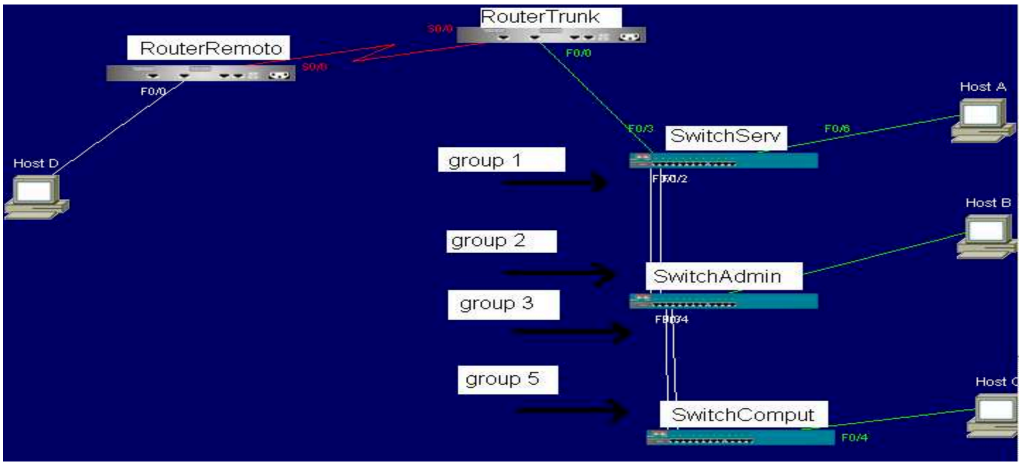

Figura 3 Puertos que forman parte de los grupos.

Figura 4 switches y routers utilizados en las pruebas, todos de marca CISCO.

Además se hizo un análisis de mercado llegando a la conclusión que los equipos CISCO son los más económicos para implementar este tipo de red, complementando con esto las pruebas en las cuales llegamos a la conclusión que el protocolo de enrutamiento EIGRP que es propietario de CISCO es el más idóneo para manejar la conectividad de los dispositivos.

Cuadro comparativo entre las diferentes ofertas.				
	opción 1 MAINT	**opción 2 MAINT**	**COMWARE**	**ANDEANTRADE**
Configuración	600 USD	600 USD	100 USD la hora	300 USD
Equipo	1745,88 USD	3893,32 USD	1890 USD	1600 USD
Mantenimiento	300 USD	600 USD	100 USD la hora	400 USD
Garantía	1 año	1 año	1 año	1 año
Adicionalmente por 250 dólares se puede contar con el servico de Smartnet solo en CISCO. ANDEANTRADE nos ofrece equipos CISCO. MAINT en sus dos propuestas nos presenta equipos NORTEL. COMWARE en su propuesta nos ofrece equipo Enterasys.				

Tabla II Cuadro comparativo de las propuestas.

CONCLUSIONES

1. Se escogió al protocolo EIGRP propietario de **CISCO** como el más indicado para trabajar en una red de este tipo, debido, que al ser un protocolo híbrido, combina lo mejor de los protocolos de estado de enlace y de los protocolos vector distancia, permite a cada router conocer la topología de toda la red, las actualizaciones no inundan la red ya que al ser tipo multicast y solo enviar los cambios no consume todo el ancho de banda de la red, está en constante comunicación con los routers que son partes de la red a través de paquetes que no consumen mucho ancho de banda del enlace y ante cualquier cambio topológico repentino, la red converge rápidamente, debido que las tablas que permiten escoger la mejor ruta están almacenada en la RAM, además EIGRP es multiprotocolo, y puede redistribuir rutas con routers que manejan IGRP.

2. Se escogió trabajar con una red de clase **B** porque nos permite tener subredes con mayor cantidad de usuarios que nos brinda la clase C, adicional a esto nos permite tener gran cantidad disponible de subredes adicionales para una futura ampliación del instituto.
3. Etherchannel propietario de **CISCO** es un método que permite tener varios puertos asociados como uno solo y si uno de ellos falla, pues la comunicación del enlace no se corta, ya que tenemos a los otros de respaldo, este es un método de redundancia muy utilizado, cuando se tiene varios switches en cascada. Por ejemplo si por cada puerto estuviésemos transmitiendo a 100 Mbps, y creáramos un etherchannel con dos puertos, lograríamos transmitir a 200 Mbps.

4. Se escogió trabajar con ACLS, porque son muy útiles para restringir el tráfico hacia recursos y aplicaciones dentro de la red a personas no autorizadas, para que no saturen el ancho de banda de la red, además prohíbe el acceso hacia una red o subred a personas externas y/o ajenas a la organización. Cuando se trabajan con ACLS extendidas, se hacen sentencias más selectivas, en lo que respecta a la aceptación o negación de tráfico. Se debe siempre tener presente si queremos bloquear el tráfico entrante o saliente de un interfaz.

5. Los equipos deben de manejar los mismos protocolos para poder comunicarse.

6. La configuración de los equipos debe de estar almacenada como información de respaldo en un servidor TFTP, para contar con los comandos y configuraciones ante una falla de funcionamiento de los equipos como reseteos repentinos ocasionados por fallas eléctricas u otros factores ajenos a la organización.

7. Una comunicación troncalizada, es más eficiente, tanto en el ahorro de puertos en los equipos activos como en el manejo de tráfico de la red.

REFERENCIAS

1. www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

2. www.cisco.com/warp/public/537/6.html

3. www.cisco.com/univercd/cc/td/ doc/product/lan/cat5000/rel_5_2/config/vtp.htm

4. www.itlp.edu.mx/publica/ revistas/revista_isc/actual/**vlan**.htm
5. es.wikipedia.org/wiki/Trunking_(red)

6. www.cisco.com/warp/public/473/21.html

7. www.cisco.com/univercd/ cc/td/doc/cisintwk/ito_doc/**rip**.htm

8. www.cisco.com/univercd/ cc/td/doc/cisintwk/ito_doc/**igrp**.htm

9. www.cisco.com/univercd/cc/ td/doc/cisintwk/ito_doc/en_igrp.htm

10. www.ciscopress.com/articles/article.asp?p=27839

11. www.cisco.com/univercd/cc/td/doc/
product/software/ios122/122cgcr/fiprrp_r/1rf**rip**.htm

12. www.cisco.com/univercd/cc/td/doc/product/
rtrmgmt/sw_ntman/cwsimain/cwsi2/cwsiug2/vlan2/stpapp.htm

13. www.cisco.com/univercd/cc/td/doc/ product/lan/cat5000/rel_5_2/config/spantree.htm

14. www.cisco.com/univercd/cc/td/doc/ product/lan/cat5000/rel_5_2/config/channel.htm

15. www.**cisco**.com/warp/public/cc/pd/rt/**2600**/index.shtml

16. www.**cisco**.demos.su/routers/**2600**.html

17. nfo.**cisco**.de/global/DE/solutions/ smb/produkte/**cisco_2950**_catalyst.pdf

18. www.ciscopress.com/articles/ article.asp?p=29803&seqNum=3 - 35k

19. www.cisco.com/en/US/products/hw/switches/
ps663/products_security_notice09186a0080264647.html - 21k –

20. www.ciscopress.com/articles/article.asp?p=29803 - 33k