MEJORANDO LA SEGURIDAD DE LAS REDES A PARTIR DE LA IMPLEMENTACIÓN DE VLANS

SYLVINE GARCÍA PACHECO.

ORLANDO GUETTE MONTALVO.

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR.

INGENIERÍA DE SISTEMAS.

CARTAGENA.

2008.

MEJORANDO LA SEGURIDAD DE LAS REDES A PARTIR DE LA

IMPLEMENTACIÓN DE VLANS

SYLVINE GARCÍA PACHECO.

ORLANDO GUETTE MONTALVO.

Monografía presentada para obtener el Titulo de Ingeniero de Sistemas.

Director:

Ing. Roberto Mercado.

Ingeniero Electrónico.

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR.

INGENIERÍA DE SISTEMAS.

CARTAGENA.

2008.

Nota de Aceptación:

_____

_____

_____

_____

_____

Presidente del Jurado:

_____

Jurado:

_____

Jurado:

_____

DEDICATORIA:

Ésta tesis la dedicó con todo mi amor y cariño a ti Dios que me diste la oportunidad de vivir y de regalarme una maravillosa familia.

Con el mayor de mis afectos, principalmente a mis padres que me dieron la vida y han estado conmigo en todo momento a pesar de las adversidades. Gracias por todo papá y mamá, gracias por darme una carrera para mi futuro y por creer en mí a pesar de mis fallas y errores; aunque hemos pasado momentos difíciles siempre han estado apoyándome y brindándome el más sincero y desinteresado de los amores, por todo esto y por mucha más razones les agradezco infinitamente y de corazón el que estén a mi lado. Los amo con toda mi alma y esta monografía que me llevo más de seis meses realizarla es para ustedes, aquí está el fruto de mi trabajo, esfuerzo y sacrificio.

A mi hermana Melissa, gracias por estar conmigo y apoyarme siempre, te quiero mucho.

Abuelita, muchas gracias por estar conmigo durante estos 21 años de vida, enseñándome y compartiendo conmigo tantas experiencias de vida, aconsejándome y alcahueteándome en todo momento. Solo quiero darte las gracias por estar conmigo en este día tan especial, por brindarme tu apoyo y amor incondicional durante todo este tiempo, los cuales me han dado la fuerza necesaria para seguir en mi camino, recuerda que eres una persona demasiado especial e importante en mi vida, Dios te conserve a nuestro lado por muchísimos años más.

Primos y Primas, Tíos y Tías, quisiera nombrarlos a todos y cada uno de ustedes, pero son muchos, eso no quiere decir que no me acuerde de cada uno, a todos los quiero mucho, y más que mi familia siempre han sido y serán mis amigos.

A todos mis amigos: Oney´s, Jorge Antonio, Luís Carlos, Kelly Paola, Mayerlis; muchas gracias por estar conmigo en todo este tiempo, donde hemos compartido momentos de alegría y de tristeza, gracias por ser mis amigos, siempre los llevaré en mi corazón.

Para ti, a pesar de que estos momentos no te encuentres junto a mí, se que nuestros corazones si lo están, porque comparten un gran sentimiento de afecto; hoy te dedicó esta tesis con todo mi corazón porque tuviste y tienes los mismos sueños que yo, y junto a ti aprendí muchas cosas que me sirvieron para forjar mi camino. A pesar de los momentos difíciles y de las adversidades siempre estuviste allí para mí, al igual que yo para ti y siempre vas hacer una

persona muy especial en mi vida. Nunca te olvidaré, siempre estarás en mi mente y en mi corazón, y mi cariño irá contigo donde quiera que vayas.

A mis profesores por confiar en mí, por tenerme la paciencia necesaria, gracias por apoyarme en los momentos difíciles. Agradezco a Dios el haber tenido unos profesores tan preparados en lo académico, como en lo humano como ustedes.

A Zeus Tecnología S.A. y a los Ing. Juan Carlos Otoya e Ing. Fernando Alcalá, por darme la oportunidad de hacer parte de su maravillosa empresa mucho antes de obtener el titulo de Ingeniero de Sistemas. Gracias porque con esa oportunidad pude aprender muchas cosas tanto a nivel profesional, como a nivel personal, que me sirvieron tanto para el desarrollo de mi carrera, como para mi crecimiento como persona.

No puedo despedirme sin antes decirles, que sin ustedes a mi lado no lo hubiera logrado, tantas desveladas sirvieron de algo y aquí esta el fruto. Les agradezco a todos ustedes con toda mi alma el haber llegado a mi vida y el compartir tantos momentos especiales, tanto felices, como tristes, pero son estos últimos los que nos hacen crecer como personas y valorar a los seres que nos rodean, los quiero mucho y nunca los olvidaré.

“Es la hora de partir, la dura y fría hora que la noche sujeta a todo horario.”

(Pablo Neruda).

Sylvine García Pacheco.

DEDICATORIA:

Este trabajo de tesis está enteramente dedicado a toda mi familia en especial a mis padres. Gracias por atreverse a confiar en mí; es obvio que sin ustedes este sueño nunca hubiera podido ser completado. Sencillamente, ustedes son la base de mi vida profesional y toda la vida les estaré agradecido. Realmente no hay palabras que logren expresar lo mucho que quiero agradecerles.

A Dios por demostrarme tantas veces su existencia y con ello darme fuerzas para salir adelante de cada tropiezo.

A mis padres por su determinación, entrega y humildad que me han enseñado tanto, mis abuelos por ser el mí perfecto ejemplo del amor eterno y mis hermanos de sangre, Walter y Wilfran, por sus enseñanzas y porque siempre alimentan mi alma.

A mis amigos, los que han pasado y los que se han quedado, porque todos ustedes han sido tantas veces parte importante de mi vida, han marcado mi existir de alguna forma y me han abierto los ojos al mundo.

A mis profesores y profesoras que me enseñaron números y letras y a todos los que mi cabeza no pudo extraer de mi memoria esta noche.

Orlando Guette Montalvo.

Cartagena de Indias, D. T y C, 4 de Febrero de 2008.

Señores:

Comité Facultad Ingeniera de Sistemas.

Universidad Tecnológica de Bolívar.

La Ciudad.

Apreciados Señores:

Cordialmente me permito informarles que he llevado a cabo la dirección del trabajo de grado de los estudiantes **SYLVINE GARCÍA PACHECO** y **ORLANDO GUETTE MONTALVO**, titulado: **MEJORANDO LA SEGURIDAD DE LAS REDES A PARTIR DE LA IMPLEMENTACIÓN DE VLANS.**

Atentamente,

_____

ING. ROBERTO MERCADO.

Cartagena de Indias, D. T y C, 4 de Febrero de 2008.

Señores:

Comité Facultad Ingeniera de Sistemas.

Universidad Tecnológica de Bolívar.

La Ciudad.

De la manera más atenta, no permitimos presentar a su consideración y aprobación, el trabajo de grado titulado: **MEJORANDO LA SEGURIDAD DE LAS REDES A PARTIR DE LA IMPLEMENTACIÓN DE VLANS** elaborado por **SYLVINE GARCÍA PACHECO** y **ORLANDO GUETTE MONTALVO**.

Esperamos que el presente trabajo se ajuste a las expectativas y criterios evaluativos de la Universidad para los trabajos de grado.

Agradeciendo de antemano su colaboración.

Cordialmente,

_____ _____

SYLVINE GARCÍA PACHECO. **ORLANDO GUETTE MONTALVO.**

CC: 1.047.378.443 DE CARTAGENA. CC: 73.194.363 DE CARTAGENA

AUTORIZACIÓN

Cartagena de Indias, D. T y C, 4 de Febrero de 2008.

Yo, **SYLVINE GARCÍA PACHECO,** identificada con número de cedula 1.047’378.443 de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi trabajo de monografía y publicarlo en el Catalogo Online de la biblioteca.

_____

SYLVINE GARCÍA PACHECO.

CC: 1.047.378.443 DE CARTAGENA

AUTORIZACIÓN

Cartagena de Indias, D. T y C, 4 de Febrero de 2008.

Yo, **ORLANDO GUETTE MONTALVO,** identificado con número de cedula 73.194.363 de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi trabajo de monografía y publicarlo en el Catalogo Online de la biblioteca.

_____

ORLANDO GUETTE MONTALVO.

CC: 73.194.363 DE CARTAGENA

TITULO DE LA MONOGRAFÍA:

MEJORANDO LA SEGURIDAD DE LAS REDES A PARTIR DE LA

IMPLEMENTACIÓN DE VLANS.

ÁREA DE INVESTIGACIÓN:

TELECOMUNICACIONES Y SEGURIDAD EN REDES.

COBERTURA DE LA INVESTIGACIÓN:

La cobertura de la investigación que se realizará será a nivel internacional, puesto que las VLANs es un concepto que ha surgido de un conjunto de soluciones propuestas por los mayores distribuidores de equipamento de Redes de Área Local para el proceso de conmutación de las mismas, con las que cualquier empresa a nivel mundial podría mejorar la Seguridad Informática de la organización con recursos básicos y siempre necesarios para la segmentación de trafico dentro la red.

CAMPO DE INVESTIGACIÓN:

Esta monografía va dirigida a Proveedores de Tecnología de Redes y Telecomunicaciones, a los Forum organizados por Autoridades Especializadas en Tecnologías de Información, la Academia Cisco en general, Instituciones Educativas y Comunidad Estudiantil, y a todos los Clientes o cualquier persona interesada en adquirir conocimientos sobre el mejoramiento de la seguridad en redes a partir del uso del uso e implementación de las VLANs.

ESTADO ACTUAL:

Con los procesos de Reingeniería de empresas y de Downsizing, y con las nuevas necesidades de independencia, autonomía y fluidez entre grupos de trabajo, se requieren nuevas facilidades y más dinámicas para realizar cambios en las redes.

Hoy día, las Redes Virtuales combinan mayores anchos de banda, facilidades de configuración y potencial de crecimiento, lo que ayudará a que se conviertan en un Standard en los entornos corporativos. Además,

En la actualidad, las implementaciones de tecnologías de Redes Virtuales no son interoperativas entre diferentes productos de diversos fabricantes y muchos de estos fabricantes intentan buscar soluciones adecuadas para lograr dicha interoperatividad, y por ello, una gran ventaja de las soluciones basadas en software es que podrán ser adaptadas a las normalizaciones.

Un punto a destacar es que la tecnología ATM prevé, como parte importante de sus protocolos, grandes facilidades para las Redes Virtuales, lo que sin duda equivaldrá a grandes ventajas frente a la competencia para aquellos equipos que actualmente ya soportan sistemas VLANs.

El futuro es claro respecto de este punto: Las características de las VLANs formarán parte, en breve, de todos los equipos que se precien de querer ser competitivos, además de que se hacen necesarios para el diseño de LANs seguras.

DESCRIPCIÓN DEL PROBLEMA:

Mientras las amenazas a la seguridad de la información de las empresas e individuos se centran en la protección contra lo evidente, los atacantes han hecho grandes adelantos en la sofisticación de sus amenazas. Ello debería ocupar a toda la industria y así sucede, sin embargo, los riesgos no disminuyen y, dadas las cifras, el peligro mayor proviene del interior de las empresas.

El asunto es más o menos claro: porcentajes que van de 70% a 80% de los ataques corresponden a los que se hicieron desde el interior de las empresas. Casi todos responden a esquemas hoy conocidos como ataques hombre en medio o man in the middle.

El problema mayor es que los resultados, de igual forma, pueden ser más letales que incluso los ataques perpetrados desde el exterior de las empresas. Así las cosas, asegurar y proteger el perímetro y los puestos de trabajo es insuficiente y hay que tomar medidas en cuanto a la circulación del tráfico en la red.

Por otro lado, cada día las aplicaciones requieren mayores anchos de banda para transferir grandes cantidades de información a través de la LAN, pues en las LAN basadas en ancho de banda compartido (configuradas mediante concentradores y enrutadores) los usuarios comparten un único canal de comunicaciones, de modo que todo el ancho de banda de la red se asigna al equipo emisor de información quedando el resto de equipos en situación de espera. En este tipo de Red Local los dominios de Broadcast se implementan de una forma muy simple, cada concentrador es un dominio de Broadcast.

Actualmente la técnica más utilizada para aumentar anchos de banda en las LANs es la conmutación (manejada mediante *switches)*. Con los switches se pueden separar o eliminar los dominios de colisión por puerto o también se puede aplicar microsegmentación en la LAN a través de la implementación de VLANs.

En las redes basadas en ancho de banda compartido, los enrutadores son esencialmente dispositivos para interconectar dominios de Broadcast. Pero con redes basadas en Switches se necesitar proveer esta función de otra forma, por lo que ambas problemáticas: Seguridad y Ancho de Banda son los pilares de los que surge esta investigación.

OBJETIVOS:

OBJETIVO GENERAL:

Investigar como se puede mejorar la seguridad de las redes a partir del uso de las VLANs.

OBJETIVOS ESPECÍFICOS:

- Entender con claridad el funcionamiento de las VLAN, y el del Enlace Troncal.
- Especificar los posibles ataques contra las VLANs, causales, consecuencias y como prevenirlos.
- Comprender como las ACLs y la implementación de Seguridad Perimetral, se complementa con el uso de las VLANs para el mejoramiento de la Seguridad en la LAN.

JUSTIFICACIÓN:

Las sociedades avanzadas de fines del siglo XX son denominadas frecuentemente sociedades de la información, pues el volumen de datos que es procesado, almacenado y transmitido es inconmensurablemente mayor que en cualquier época anterior. Actualmente en el siglo XXI la información es poder, por ello las organizaciones la valoran mucho. De hecho, en la actualidad, las organizaciones consideran que la información es un bien más de sus activos y en muchos casos, prioritario sobre los restantes de la organización.

Pero gran parte de esos datos que nosotros, o las entidades de nuestra sociedad, manejamos, han sido tratados, sea durante su proceso, o almacenamiento, o transmisión, mediante las llamadas tecnologías de la información, entre las que ocupa un lugar focal la informática. Consiguientemente, la seguridad de las tecnologías de información, y por ende la informática, se convierte en un tema de crucial importancia para el continuo y espectacular progreso de nuestra sociedad, e incluso para su propia supervivencia.

Por otro lado, la evolución en los últimos años de las redes informáticas y fundamentalmente de Internet, han sido el factor fundamental que ha hecho que la Seguridad Informática y sus estándares cobrasen una importancia vital en el uso de sistemas informáticos conectados.

Estando entonces en la era de la información, cada día se hace más necesario, preservar y proteger la información que circulan dentro y fuera de las empresas, es por eso que actualmente los Ingenieros de Sistema de las organizaciones buscan soluciones tecnológicas que permitan salvaguardar los datos de mismas, previendo no solo los ataques externos a los que se vean expuestos, sino también los ataques internos que últimamente han tomado mucho auge; por todas esta razones parte de esta monografía va dirigida a como mejorar la seguridad de las redes LANs a partir del uso de la técnica de VLANs y de que manera nos ayudan como complemento la aplicación de la Seguridad Perimetral en una red existente. Por otro lado, y con el paso del tiempo las aplicaciones requieren mayores anchos de banda para transferir grandes cantidades de información a través de la LAN y por ende se hace necesario el uso de redes conmutadas y la implementación de VLANs, las cuales traen consigo grandes beneficios, entre ellos: rapidez, confiabilidad, pero sobre todo ampliación del ancho de banda, ya que el dispositivo puede capturar toda la capacidad de la red cuando sea necesario, debido a que los usuarios comparten un único canal de comunicaciones, de modo que todo el

ancho de banda de la red se asigna al equipo emisor de información quedando el resto de equipos en situación de espera; por todos estos motivos, parte de esta monografía va dirigida a comprender el funcionamiento de las VLANs.

TIPO DE INVESTIGACIÓN:

Esta investigación esta enmarcada desde diferentes ópticas, teniendo en cuenta el desarrollo de la misma, entre ellas, encontramos la parte Histórica donde se muestra un poco la parte evolutiva, de desarrollo e implementación de las VLANs; la parte Descriptiva donde se detallan entre otros aspectos características, funcionalidades y tipologías de conceptos relativos a las VLANs y a las ACLs y por ultimo encontramos la parte de Desarrollo Tecnológico en la cual se tiene algunas de las características más relevantes de los equipos de ultima generación y los aportes más significativos que las VLANs han realizado para el mejoramiento de la seguridad en las redes.

TABLA DE CONTENIDO:

Pág.

5. SEGURIDAD PERIMETRAL:

LISTA DE FIGURAS:

Pág.

RESUMEN:.

En la medida que las redes han crecido en tamaño y complejidad, muchas compañías han comenzado a prestar atención e implementar Redes Virtuales de Área Local (VLAN, Virtual Area Networks) para proveer una forma de estructurar este crecimiento de forma lógica.

Básicamente una VLAN es un agrupamiento lógico de dispositivos o usuarios, ya sea por función, departamento o tipo de aplicación independiente de su ubicación física, conformando un segmento de red. Un dominio de difusión se da cuando un grupo de dispositivos en la red envían y reciben mensajes de difusión entre ellos.

Por lo general, en una red hay tantos dominios de difusión, como tantos número de VLANs haya, es decir, los equipos que estén agrupados en una misma VLAN, hacen parte de un mismo dominio de difusión.

típica todo lo que se encuentra de un lado del router pertenece al mismo dominio de difusión. En un switch donde haya implementado VLANs contiene múltiples dominios de difusión.

A continuación se listan algunas de las razones comunes por las que una compañía quisiera implementar VLANs:

- **Seguridad:** Separando sistemas que tenga información sensible del resto de la red disminuye las probabilidades de que las personas no autorizadas tengan acceso a dicha información.
- **Aplicaciones/Proyectos Especiales**: La gestión o el trabajo en una aplicación especializada puede simplificarse por medio de una VLAN que agrupen a todos los nodos involucrados.
- **Desempeño/Ancho de Banda:** El ancho de banda se mejora, porque al segmentar la red por VLANs, separo los dominios de difusión, por ende “tengo control” sobre las difusiones y no permito que se difundan en toda la red.
- **Implementación de Políticas de Tráfico:** Al tener identificado un número y tipo de usuarios puedo aplicarles políticas de control como las ACLs, donde se definan políticas de uso de Internet, permisos, ancho de banda permitido, etc.
- **Tareas Departamentales/Específicas** Las empresas pueden desear VLANs definidas para los departamentos que son usuarios pesados de la red (tales como multimedios e ingeniería), o una VLAN entre departamentos que esté dedicada a empleados especiales (tales como gerentes o personal de venta).

Se puede crear una VLAN en la mayoría de los switches haciendo Telnet e ingresando los parámetros para la VLAN (nombre, dominio y asignación de puertos). Una vez creada la VLAN, cualquier segmento de red conectado a los puertos asignados pasarán a ser parte de dicha VLAN. Si bien se puede tener más de una VLAN en un switch, ellas no se pueden comunicar entre sí directamente en ese switch. Si pudieran, desafiaría el propósito de tener VLANs que es aislar parte de la red. Las comunicaciones entre VLANs requieren un enrutador.

Las VLANs se pueden extender a múltiples switches y se puede tener más de una VLAN por switch. Simplemente, para que una VLANs pueda estar contenida en más de un switch, es necesario que la comunicación entre los switches de haga a partir de puertos en modo trunk. Este modo se puede hacer de dos formas:

- ISL : Protocolo propietario de Cisco poco utilizado.

- 802.1Q: Técnica Estándar, que a diferencia de ISL no es un Protocolo. Es una técnica donde se observa el tag o etiqueta sobre la trama Ethernet en si., haciéndolo mucho más versátil que el primero.

Los primeros diseñadores de redes solían configurar las VLAN con el propósito de reducir el tamaño del dominio de colisión en un único segmento Ethernet, mejorando así el rendimiento.

Cuando los switches Ethernet hicieron desaparecer este problema debido a que no tienen dominio de colisión, el interés se desplazó a reducir el tamaño del dominio de difusión en la subcapa MAC.

Por otro lado, las VLAN también pueden ser utilizadas para restringir el acceso a recursos de red, independientemente de la topología física de esta. El primer suministrador de switches con soporte VLAN fue ALANTEC (familia de concentradores/switches multimedia inteligentes PowerHub), pero actualmente son muchos los fabricantes que ofrecen equipos con soluciones VLAN: Bytex (concentrador inteligente 7700), Cabletron (ESX-MIM), Chipcom (OnLine), Lannet (MultiNet Hub), Synoptics (Lattis System 5000), UB (Hub Access/One) y 3Com (LinkBuilder).

Las VLANs funcionan en el nivel 2 (enlace de datos) del modelo OSI. Sin embargo, los administradores suelen configurar las VLANs como correspondencia directa de una red o subred IP, lo que hace que funcionen en el nivel 3 (red).

INTRODUCCIÓN:

Las Redes de Área Local Virtuales (VLANs) han surgido de un conjunto de soluciones que los fabricantes de dispositivos de Redes de Área Local (LAN) habían propuesto para la conmutación de éstas. Aunque el entusiasmo del usuario final por la implementación de las VLANs todavía no se ha mostrado, la mayoría de las empresas han empezado a buscar fabricantes que propongan una buena estrategia para su VLANs, así como que éstas sean incorporadas sobre las redes existentes, añadiendo funciones de conmutación y un software de gestión avanzado. Una de las razones de que se centre la atención sobre las VLANs ha sido el rápido desarrollo de las LANs conmutadas, hecho que comenzó en 1994/1995.

Los modelos de redes basados en la compartición de ancho de banda, presentes en las arquitecturas LAN de los primeros noventa, carecían de la potencia suficiente como para proporcionar los cada vez mayores anchos de banda que requieren las aplicaciones multimedia. En la actualidad se necesitan nuevos modelos capaces de proporcionar la potencia suficiente no sólo para satisfacer la creciente necesidad de ancho de banda, sino también para soportar un número mayor de usuarios en la red.

En las LAN basadas en compartición de ancho de banda, los usuarios comparten un único canal de comunicaciones, de modo que todo el ancho de banda de la red se asigna al equipo emisor de información quedando el resto de equipos en situación de espera. Para aumentar el ancho de banda disponible para cada usuario, se puede optar por la segmentación de sus segmentos y anillos. Ahora bien, estas técnicas no ofrecen buenas prestaciones, debido principalmente a las dificultades que aparecen para gestionar la red. Cada segmento suele contener de 30 a 100 usuarios.

La técnica idónea para proporcionar elevados anchos de banda es la conmutación; mediante esta técnica, cada estación de trabajo y cada servidor poseen una conexión dedicada dentro de la red, con lo que se consigue aumentar considerablemente el ancho de banda a disposición de cada usuario.

Las LANs basadas en compartición de ancho de banda se configuran mediante *hub, switches* y *routers*. En una LAN conmutada, la función tradicional del *router* -encaminamiento de la información en la red- pasa a ser realizada por el conmutador LAN, quedando aquél destinado a funciones relacionadas con la mejora de las prestaciones en lo que respecta a la gestión de la red. Con este nuevo papel del *router*, se pueden contener de 100 a 500 usuarios. El decremento en los precios de switches *Ethernet* y *Token Ring* ha sido uno de los principales empujes a que un buen número de empresas se inclinen por una LAN conmutada.

Sin embargo, el continúo despliegue de switches, dividiendo la red en más y más segmentos (con menos y menos usuarios por segmento) no reduce la necesidad de contenido de *broadcast* -información para gestionar la red. Las VLANs representan una solución alternativa a los *routers* con función de

gestores de la red. Con la implementación de switches en unión con VLANs, cada segmento de la red puede contener como mínimo un usuario, mientras los dominios de *broadcast* -conjunto de estaciones de trabajo conectadas a un mismo *hub o switch*- pueden contener 1000 usuarios, o incluso más. Además, las VLANs pueden enrutar movimientos de las estaciones de trabajo hacia nuevas localizaciones, sin requerimiento de reconfigurar manualmente las direcciones IP.

DESARROLLO:

1. REDES DE ÁREA LOCAL:

1.1. Definición:

Una Red de Área Local es un grupo de equipos que pueden compartir datos, aplicaciones y recursos, dichos equipos están separados por distancias de hasta unos pocos kilómetros y se suelen usar en oficinas o campus universitarios, permitiendo la transferencia rápida y eficiente de información.

1.2. Características y Generalidades:

El atributo característico y primordial de una Red de Área Local es que los dispositivos que la componen comparten los recursos del medio físico, entre ellos, el ancho de banda y otros. *"Cuando utilizamos un concentrador o hub dentro de una red, ésta se puede ver como una red de distribución hidráulica, donde las estaciones de trabajo conectadas a la misma, toman cierta cantidad de agua, y mientras más máquinas existan en esa LAN, menor será la cantidad de líquido que podrán utilizar. A este segmento de "tubería" se le puede llamar también "dominio de colisiones" "* [1]

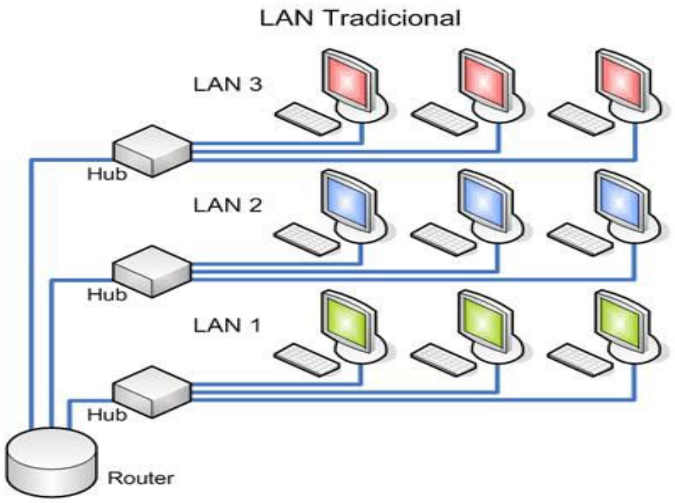

Figura 1. Red de Distribución.

Fuente: *http://wiki.glib.org.mx/index.php/WikiGlib:Ayuda*

La utilización de un switch perfecciona el rendimiento de una red, ya que este dispositivo segmenta los dominios de colisiones; básicamente

[1]VLAN: Red de Área Local Virtual, extraído de http://www.enterate.unam.mx/Articulos/2004/noviembre/vlan.htm

lo que hace un switch, es compartir el ancho de banda, por esta razón en cualquier momento dado cuando el medio este ocupado por la transmisión de información generada por alguno de los equipos de la red y en el momento en el que otro equipo perteneciente a esa misma red precise en enviar información durante ese mismo lapso de tiempo, solo lo podrá hacer cuando el medio se encuentre desocupado para evitar que los datos se encuentren y produzca una colisión, dando como resultado la destrucción del mensaje y por lo tanto tendría que enviarse nuevamente, lo que conduce a muchas retransmisiones de información y por ende mayor ocupación del canal.

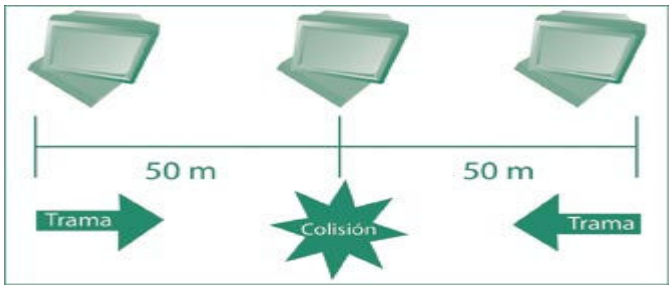

Figura 2. Dominio de Colisiones.

Fuente: http://www.enterate.unam.mx/Articulos/2004/noviembre/vlan.htm

En una LAN, cada uno de los puertos es una “carretera” asociada a cada una de las casas (equipos) dentro de la red, donde cada equipo dispone de todo el ancho de banda que la red proporciona, con el objetivo de prevenir las colisiones que pudieran existir en un medio compartido, por ello cada equipo tiene un canal individual enlazado con el punto central de distribución que es el switch.

Una condición que no puede optimizar ni el switch o el hub, es el envío de mensajes de broadcast dentro de una LAN. Estos mensajes los escuchan todos los equipos de la LAN, puesto que se está realizando una búsqueda general porque existe un paquete que va dirigido hacia alguno de los equipos de la red.

En una Red de Área Local, los mensajes de broadcast son enviados a través de cada uno de los puertos del switch o hub, ya que si un equipo requiere comunicarse o trasmitirle información a otro y este primero no sabe donde se encuentra el segundo, entonces se hace una especie de inundación de la red a través de un mensaje de búsqueda (broadcast), lo que lógicamente se traducirá en tráfico dentro de la red, además de que todos los equipos escucharan el mensaje, pero solo tendrá potestad de contestarlo el equipo a quien va dirigido el paquete, sin importar si se encuentra o no conectado dentro del switch o hub.

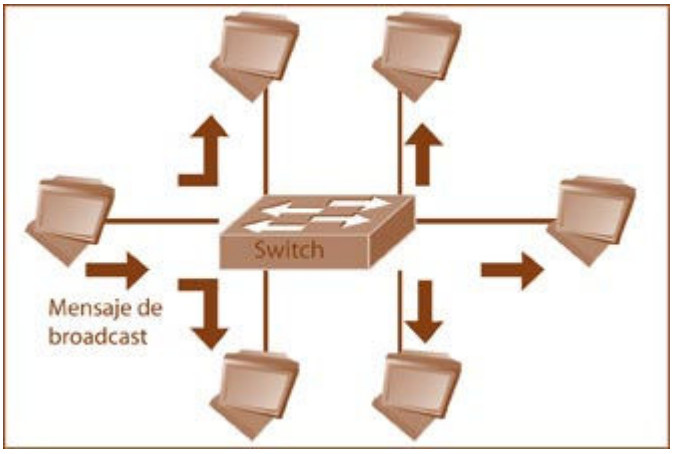

Figura 3. Dominio de Broadcast.

Fuente: http://www.enterate.unam.mx/Articulos/2004/noviembre/vlan.htm

Estos mensajes de broadcast muchas veces se convierten en tráfico innecesario e inútil para los demás equipos en la media en que si solo se requiere un equipo especifico, de igual forma se afectan en resto de equipos pertenecientes al dominio de broadcast.

Teniendo en cuenta que los grupos de trabajo en una red, por lo general, son creados considerando la asociación física de los usuarios en un mismo segmento de la red o en un mismo hub, encontramos como consecuencia directa, que estas divisiones comparten el ancho de banda y los dominios de broadcast; adicionalmente nos encontramos con la problemática de gestionar y administra la red cuando se producen cambios en los usuarios pertenecientes al grupo. Pero lo mas grave aun es que tenemos la limitante geográfica que supone que los usuarios perteneciente a un relativo grupo, deben estar situados aledañamente, por su conexión al mismo concentrador o segmento de la red.

Para solucionar dicha problemática, se creó el concepto de Redes de Area Local Virtuales (VLANS), que configuradas dentro de los switches, se encargan de dividir en distintos dominios de broadcast a un switch, con el objetivo de no afectar a los demás puertos del switch dentro de un solo dominio de broadcast, sino crear dominios más pequeños y aislar las consecuencias que pudieran generar los mensajes de broadcast a solamente algunos puertos, y afectar al menor numero de equipos posibles.

2. VLANS:

2.1. Definición y Generalidades:

Una Red de Área Local Virtual (VLAN) es un conjunto de dispositivos conectados en red, que sin importar que estén conectados en diferentes ubicaciones físicas pertenecen a una misma Red de Área Local.

Para poder realizar este proceso, se hace indispensable la utilización de un switch, el cual adicionalmente mejora el rendimiento de la red en los siguientes aspectos:

- Aísla los dominios de colisión por cada uno de los puertos.
- Dedica el ancho de banda a cada uno de los puertos y por lo tanto a cada equipo.
- Aísla los dominios de broadcast.
- Proporciona seguridad debido a que a la asignación que se realiza de los puertos a las VLAN.
- Controla y administra de manera idónea de las direcciones IP, debido a que se asignan bloques de IPs para cada VLAN, evitando la manipulación manual del usuario final y la duplicidad de direcciones IP que podrían generan conflictos mas adelante.
- No importa la ubicación física de los usuarios finales, pues si estamos configurados dentro de una VLAN, en donde nos encontremos conectados dentro del edificio de oficinas, si estamos configurados en una VLAN, nuestro grupo de trabajo podrá “vernos” y podremos compartir el ancho de banda de nuestro segmento de red, así mismo como datos, aplicaciones y recursos.

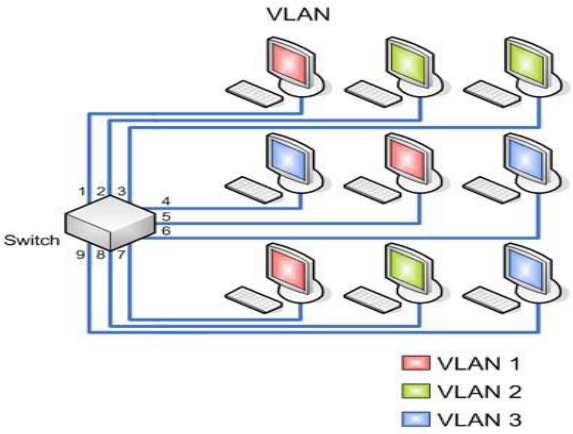

Figura 4. VLAN

Fuente: http://wiki.glib.org.mx/index.php/WikiGlib:Ayuda.

En la figura 4 podemos observar los elementos de la implementación de una VLAN y además para nuestro interés en la capa 2, se encuentran los cuatro tipos de VLANs principales que se explicaran a continuación.

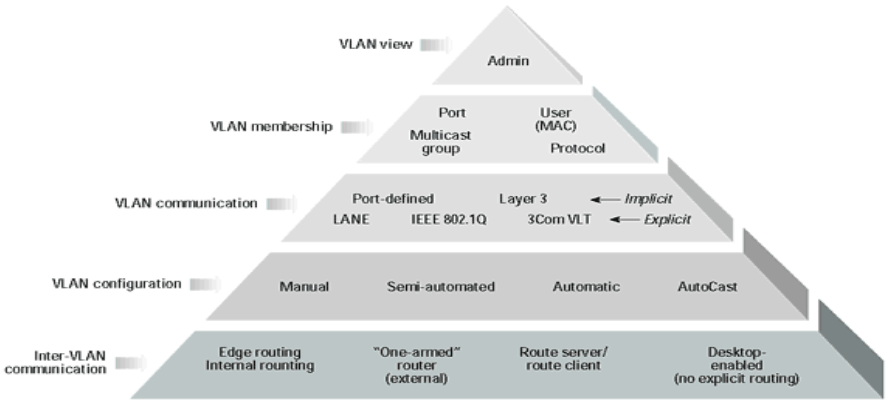

Figura 5. Elementos de la implementación de una VLAN.

Fuente: http://www.lcc.uma.es/~eat/services/rvirtual/rvirtual.html**.**

2.2. El Estándar y su Funcionamiento:

Los esquemas VLAN funcionan mediante la agrupación de segmentos realizada de una forma lógica en lugar de física, aunque las Redes Virtuales continúan compartiendo las características de los grupos de trabajo y sus dominios de broadcast. Al realizará una agrupación lógica de los usuarios, obtenemos como ventaja que podemos realizar una distribución completa a través de la red, inclusive si los equipos se

encuentran situados en concentradores diferentes, con lo que logramos la movilidad física de los usuarios, al tiempo que continúan perteneciendo al mismo grupo lógico y obtenemos como resultado inmediato el ensanchamiento del ancho de banda en el grupo lógico.

Además, al poder distribuir a los usuarios en diferentes segmentos de la red, podemos situar bridges y routers entre ellos, separando segmentos con diferentes topologías y protocolos, en función tanto de las instalaciones existentes como del ancho de banda que cada uno necesite, por su ocupación específica en el grupo, lo que nos permite mantener la seguridad en la red, y realizar una administración mucha mas especifica de la misma, en la medida que podemos permitir que el tráfico de una VLAN entre y salga desde y hacia otras VLAN y/o redes.

"Las Redes Virtuales nos permiten que la ubicuidad geográfica no se limite a diferentes concentradores o plantas de un mismo edificio, sino a diferentes oficinas intercomunicadas mediante redes WAN o MAN, a lo largo de países y continentes, sin limitación ninguna más que la impuesta por el administrador de dichas redes"[2]

Las LANs Virtuales (VLANs) son congregaciones, dadas por software, de estaciones LAN que se comunican entre sí como si estuvieran conectadas al mismo cable, inclusive estando ubicadas en segmentos distintos de una red de edificio o de campus; por lo que podríamos decir que una Red Virtual es la tecnología que permite dividir el ámbito lógico de la red, de su distribución física mediante la creación de grupos de usuarios (como definición lógica), para la colaboración en sistemas informáticos de redes, simplificando la tarea de administrar los movimientos, adiciones y cambios del usuario dentro de la LAN.

Realizando este análisis en una empresa dedica al Desarrollo de Software, que este compuesta por los Departamentos de Administración, Contabilidad, Desarrollo, Pruebas y Soporte y Auditoria, si trasladamos al Departamento de Desarrollo para otro edificio en pro del bienestar de los desarrolladores, debido a que las múltiples presentaciones del Departamento de Ventas no permite la concentración de los mismos, este cambio físico seria transparente para el usuario final gracias a la visión lógica de la red virtual, adicionalmente, se reduciría notablemente el tiempo y los datos asociados con los movimientos físicos, permitiendo que la red mantenga su estructura lógica sin costos económicos extras, reduciendo la tarea netamente al plano de administración de la red y al control de los software destinados para dicho fin, al tiempo que los centros de cableado permanecen seguros y a salvo de interrupciones.

Todo el desarrollo y políticas diseñadas alrededor del funcionamiento e implementación de VLANs fueron elaborados por la IEEE (Instituto de

[2] Redes Virtuales: El primer paso hacia la ubicuidad geográfica, extraído de http://www.consulintel.es/Html/Tutoriales/Articulos/vlan.html

Ingenieros Eléctricos y Electrónicos) y especificadas en el estándar IEEE 802.1Q.

"En el estándar 802.1Q se define que para llevar a cabo esta comunicación se requerirá de un dispositivo dentro de la LAN, capaz de entender los formatos de los paquetes con que están formadas las VLANs. Este dispositivo es un equipo de capa 3, mejor conocido como enrutador o router, que tendrá que ser capaz de entender los formatos de las VLANs para recibir y dirigir el tráfico hacia la VLAN correspondiente". [3]

El protocolo IEEE 802.1Q fue un propósito del grupo de trabajo 802 de la IEEE para elaborar un componente que permitiera a múltiples redes compartir transparentemente el mismo medio físico sin complicaciones de interferencia, por lo que se convirtió en el nombre actual del estándar establecido en este proyecto y que se usa para definir el protocolo de encapsulamiento usado para implementar el mecanismo de Trunking en redes Ethernet.

2.3. Tipos de VLAN, Ventajas y Desventajas:

Existen varias formas en que se puede definir una VLAN, pero entre las principales y más importantes encontramos: las basadas en puertos, las basadas en MAC, las VLANs de capa 3 y las basadas en reglas.

2.3.1 VLANs Basadas en Puertos:

Consisten en una agrupación de puertos físicos que pueden estar conectados en uno conmutador o varios switches, donde la asociación de los equipos a la VLAN se realiza teniendo en cuenta los puertos a los que están conectados físicamente. Este método es la forma más común de definir la pertenencia a una VLAN.

En una red empresarial podríamos identificar esta práctica con el esquema descrito en la figura 5, donde se contempla la utilización de múltiples switches por ejemplo, los puertos 1 y 2 del conmutador 1 y los puertos 4,5,6 y 7 del conmutador 2 forman la VLAN A; mientras que los puertos 3,4,5,6,7 y 8 del conmutador 1 combinados con los puertos 1,2,3 y 8 del conmutador 2 configuran la VLAN B).

.

[3] http://www.enterate.unam.mx/Articulos/2004/noviembre/vlan.htm

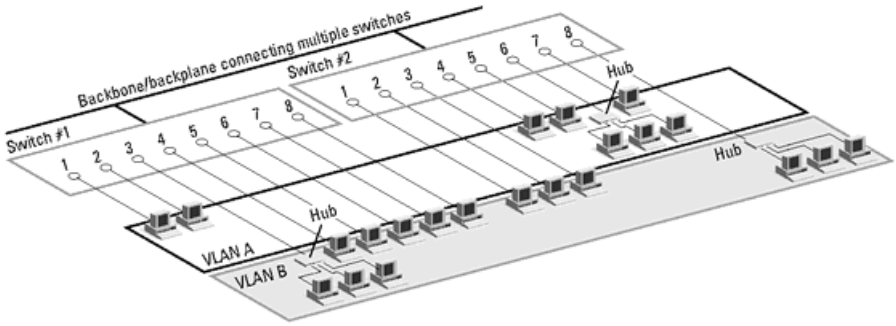

Figura 6. VLANs basadas en Puertos.

Fuente: http://www.lcc.uma.es/~eat/services/rvirtual/rvirtual.html.

Ventajas:

- Facilidad de movimientos y cambios.
- Microsegmentación y reducción del dominio de Broadcast.
- Multiprotocolo.

Desventajas:

- Dificultad en la administración de la red, en la medida que cuando surge un cambio en las estaciones de trabajo, se hace necesaria la reconfiguración del puerto del switch al que esta conectado el usuario.

2.3.2. VLANs Basadas en MAC:

Consiste en la agrupación de las estaciones de trabajo en una VLAN, teniendo en cuenta sus direcciones MAC. Se dice que este tipo de VLANs son orientadas al usuario, en la medida en que el administrador de la red puede reubicar ésta estación de trabajo físicamente, mientras mantiene su permanencia en la VLAN, ay que las direcciones MAC, se encuentran directamente implementadas sobre las Tarjetas de Interface de la Red (NIC).

MAC	VLAN
12.15.89.bb.1d.aa	1
12.15.89.bb.1d.aa	2
aa.15.89.b2.15.aa	2
1d.15.89.6b.6d.ca	2
12.aa.cc.bb.1d.aa	1

Figura 7. VLANs basadas en Direcciones MAC.

Fuente: http://www.textoscientificos.com/redes/redes-virtuales

Ventajas:

- Facilidad de movimientos: No es necesario en caso de que una terminal de trabajo cambie de lugar la reconfiguración del switch.
- Multiprotocolo.
- Se pueden tener miembros en múltiples VLANs.

Desventajas:

- Problemas de rendimiento y control de broadcast, debido a que el tráfico de paquetes de tipo multicast y broadcast se propagan por todas las VLANs de la red.
- Complejidad en la administración, debido a que inicialmente a todos los usuarios se les deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo.
- Degradación del método de compartición de información mediante switches entre miembros de la VLAN cuando la implementación es a gran escala.

2.3.3. VLANs de Capa 3:

Tienen en cuenta el tipo de protocolo o direcciones de la capa de red (direcciones lógicas), para determinar la pertenencia a una VLAN.

Protocolo	VLAN
IP	1
IPX	2
IPX	2
IPX	2
IP	1

Figura 8. VLANs de Capa 3.

Fuente: http://www.textoscientificos.com/redes/redes-virtuales

Ventajas:

- Permiten la segmentación por tipo de protocolo, lo que puede parecer interesante para los administradores que como estrategia de VLAN realizan sus configuraciones basados en servicios o aplicaciones.

- Eliminan la necesidad de marcar las tramas para comunicar usuarios de la red mediante switches, disminuyendo los gastos de transporte.
- Para los usuarios de TCP/IP se puede realizar movilidad de sus estaciones sin tener que reconfigurar cada una de las direcciones de red de la misma.

Desventajas:

- Problemas de rendimiento y control de broadcast, debido a que en las búsquedas efectuadas en las tablas de pertenencia se consume mucho mas tiempo que buscar una dirección MAC en una trama y es por esta misma razón que los switches que usan información de la capa 3 para la definición de VLANs son generalmente más lentos que los que usan información de la capa 2.
- No soporta protocolos de nivel 2, ni protocolos dinámicos, siendo mucho mas efectivas en el trato con TCP/IP, pero mucho menos efectivas con protocolos como IPX, DECnet AppleTalk, que no implican configuración manual. Además tienen la dificultad al tratar con protocolos no enrutables como NetBIOS (estaciones finales que soportan protocolos no enrutables no pueden ser diferenciadas y, por tanto, no pueden ser definidas como parte de una VLAN).

2.3.4. VLANs Basadas en Reglas:

Es un esquema de trabajo que consiste en la combinación de varios criterios para la definición de los miembros pertenecientes a cada VLAN de acuerdo a las necesidades específicas de los gestores de la red. Una vez que el conjunto de criterios que constituyen la política a aplicar se ejecuta en la VLAN, ella misma realiza una especia de seguimiento sobre los movimientos de los usuarios en la red.

Las ventajas de este tipo de implementación saltan a la vista, pero depende mucho de la composición de las políticas, por lo que no se pueden detallar a ciencia cierta así mismo como las desventajas dentro de las cuales solo se podría considerar la complejidad de administración de dichas políticas.

Adicional a los tipos de VLANs que hemos observado con anterioridad podemos encontrar los siguientes:

2.3.5. VLANs de Puerto Central:

En este tipo de VLANs todos los nodos de una VLAN se conectan al mismo puerto del switch.

2.3.6. VLANs Estáticas:

En este tipo de VLANs, los puertos del switch están previamente preasignados a las estaciones de trabajo.

2.3.7. VLANs por Direcciones IP:

Este tipo de VLANs se basan en el encabezado de la capa 3 del Modelo OSI, donde las direcciones IP de los servidores de VLAN establecidos, no operan como router sino que lo hacen para realizar un mapeo de las direcciones IP autorizadas para entrar en la VLAN.

Ventajas:

- Facilidad en los cambios de estaciones de trabajo, ya que : con la asignación de una dirección IP estática no es necesario reconfigurar el switch.

Desventajas:

- El tamaño de los paquetes enviados es menor que en el caso de utilizar direcciones MAC.
- Perdida de tiempo en la lectura de las tablas.
- Complejidad en la administración, debido a que inicialmente todos los usuarios deberían configurarse de forma manual.

2.3.8. VLANs por Nombre de Usuario:

Este tipo de VLANs se fundamentan en la autenticación del usuario.

Ventajas:

- Facilidad de movimiento de los integrantes de la VLAN.
- Multiprotocolo.

Desventajas:

- Administración de las tablas de usuarios en corporaciones muy industriosas.

2.3.9. VLANs Dinámicas (DVLANS):

"Las VLANs dinámicas son puertos del switch que automáticamente determinan a que VLAN pertenece cada puesto de trabajo. El funcionamiento de estas VLANs se basa en las direcciones MAC, direcciones lógicas o protocolos utilizados"[4].

Cuando un equipo de trabajo realiza su respectivo proceso de autenticación para conectarse a la VLAN el conmutador verifica la dirección MAC inscrita previamente por el administrador en la base de datos de las mismas y automáticamente se establece el puerto al cual corresponde por la configuración de la VLAN.

La gran ventaja del uso de las DVLANs esta relacionado con el poco trabajo de administración dentro del rack de comunicaciones cuando se cambian de lugar los equipos de trabajo o se añade uno nuevo, además de notificar de forma centralizada cuando un usuario desconocido intenta acceder en la red.

2.3.10. Redes LAN Emuladas (ELAN):

La definición de VLAN aparece asociada directamente al concepto de LAN, que es una tecnológica no orientada a conexión, pero como en el mercado, también existen muchas redes basadas en ATM, que es una tecnología orientada a conexión, surgió la necesidad de crean VLAN en redes ATM . En términos generales las VLAN ATM, se basan en direcciones ATM y haciendo una analogía con las redes LAN estas direcciones vendrían siendo las MAC, solo que con ATM se establecen circuitos virtuales permanentes.

Ventajas:

- Facilidad de administración.
- Facilidad de movimientos y cambios.
- Multiprotocolo.

Desventajas:

- Aplicable solo a Ethernet y Token Ring.
- No explota la calidad de Calidad de servicio (QoS) de ATM.

[4] Redes Virtuales VLANs extraído de http://www.textoscientificos.com/redes/redes-virtuales

2.3.11. VLANS Binding:

"Se conjugan tres parámetros o criterios para la asignación de VLANs: si el usuario es del puerto x, entonces se le asignara una VLAN correspondiente. También puede ser puerto, protocolo y dirección MAC, pero lo importante es cubrir los tres requisitos previamente establecidos, ya que cuando se cumplen estas tres condiciones se coloca al usuario en la VLAN asignada, pero si alguno de ellos no coincide, entonces se rechaza la entrada o se manda a otra VLAN."[5]

2.3.12. VLANS por DHCP:

Este tipo de VLANs están basadas en el protocolo DHCP, en el cual se asignan direcciones IP de forma dinámica a los equipos de trabajo que pertenezcan a la red y teniendo en cuenta esta acción se asigna al usuario la VLAN correspondiente, convirtiéndose en una política de última generación.

2.4. Tecnologías utilizadas para proporcionar Redes Virtuales:

Existen tres tipos de tecnologías que pueden ser utilizadas como soluciones efectivas para proporcionar Redes Virtuales, las cuales se detallaran a continuación. Estas soluciones se apoyan en la mayoría de arquitecturas de red que utilizan switches.

2.4.1. Switches de Puertos: Son concentradores con varios segmentos, los cuales proveen el máximo ancho de banda disponible de acuerdo al tipo de red y compartiendo este recurso entre todos los puertos saciados a este segmento; sus puertos son dinámicamente asociados a cualquiera de los segmentos, mediante la utilización de instrucciones de software. *"Cada segmento se asocia a un "backplane", el cual a su vez, equivale a un grupo de trabajo. De este modo, las estaciones conectadas a estos puertos pueden asignadas y reasignadas a diferentes grupos de trabajo o Redes Virtuales"*[6].

Su ventaja principal es la facilidad para la reconfiguración de los grupos de trabajo; no obstante, tienen graves restricciones, debido a que diseñados como dispositivos compartiendo un único backplane físico, por lo que todos los usuarios pertenecientes al mismo grupo de trabajo deberán estar relativamente adyacentes físicamente. Adicionalmente las VLAN sufren de conectividad con el resto de la red, ya que al segmentar los backplanes, no existe conectividad integrada entre sus propios miembros; si se quiere

[5] Clasificación de las VLAN extraído de http://esi-10-edu.shinranet.com/web_03/clasificacion.htm
[6] Redes Virtuales: el primer paso hacia la ubicuidad geográfica extraído de http://www.consulintel.es/Html/Tutoriales/Articulos/vlan.html

realizar la conectividad, se necesita un bridge o router externo, lo que genera cambios y traumatismos en la red, sin mencionar el aumento de los costos y que esta situación no soluciona la problemática de saturación del ancho de banda de la red.

2.4.2. Switches de Segmentos con Bridging: Son switches que proporcionan el ancho de banda de múltiples segmentos de red, conservando la conectividad entre dichos segmentos a través de los algoritmos tradicionales empleados en los bridges. En esta tecnología, las VLANs son grupos lógicos de nodos o en su defecto dominios de broadcast lógicos que pueden ser conectados a cualquier número de segmentos de red y recibirán todos los paquetes enviados por cualquier nodo en la VLANs, como si estuvieran conectados físicamente en el mismo segmento.

Los switches de segmentos con bridging se pueden reconfigurar mediante comandos software y modificar la estructura de la VLAN, y adicionalmente se cuenta con la ventaja de que ancho de banda repartido entre varios segmentos físicos, lo que evita la saturación del canal, puesto que los usuarios pueden ubicarse en los diferentes segmentos, con lo que se logra ampliar el ancho de banda en función del número de segmentos usados y se mantiene el concepto de grupo de trabajo.

Presenta el mismo problema de comunicación con el resto del grupo, así como lo tiene la conmutación de puertos y por consiguientes las mismas consecuencias.

2.4.3. Switches de Segmentos con Bridging/Routing: Dispositivos que manejan las características mas relevantes de los switches de segmentos con funciones de bridging, además, con funciones agregadas de routing, lo que brinda facilidades en la reconfiguración de la red, la conectividad entre VLANs y redes tanto locales como remotas, así como la posibilidad de implementar grupos de trabajo que se expandan a través de diferentes segmentos de red.

Con esta tecnología podemos evadir el recableado de la red o el cambio en direcciones de subredes, debido a la reconfiguración que se puede realizar a través del software del conmutador, permitiéndonos asignar el ancho de banda necesitado por los diferentes grupos de trabajo sin perturbar a las aplicaciones de red existentes.

Con la conmutación de segmentos con bridging/routing se soluciona el problema de comunicación con el resto de las redes que presentaban las tecnologías anteriormente relatadas, e

inclusive se puede realizar de dos formas diferentes, uno es permitiendo que algunos segmentos pertenezcan a varios grupos de trabajo, o en su defecto, por razón de las funciones de routing multiprotocolo integradas, que facilitan el tráfico incluso entre varias VLANs.

De la misma forma, hay que tener en cuenta que los modelos más avanzados de switches con funciones VLANs, soportan filtros muy sofisticados, definidos por el administrador de la red, y que le permiten establecer características relacionadas con el tráfico y la seguridad en el dominio, todo esto realizado en base a los algoritmos de bridging, y routing multiprotocolo.

2.5. Razones por las cuales una compañía quisiera implementar VLANs:

Debido al vertiginoso proceso de industrialización que ha sufrido el mundo entero durante los últimos años, las pequeñas, medianas y grandes empresas comenzaron a crecer en volumen de empleados y su complejidad estructural evolucionó de la misma forma, fue entonces cuando los administradores de sistemas de estas compañías se vio en la necesidad de buscar una manera de estructurar este crecimiento de forma lógica y comenzaron a implementar el concepto de VLAN dentro de sus redes, el cual se basa en el principio de dominio de difusión.

Un dominio de difusión es una red que recibe paquetes de difusión desde cualquiera de los nodos ubicados dentro de si misma. Si llevamos este principio al campo práctico y realizamos una analogía entre una red típica y una red donde se haya implementado VLANs, podremos notar que en la primera, todo lo que se encuentra de un lado del router pertenece al mismo dominio de difusión, mientras que en la segunda en el switch donde se haya realizado la segmentación habrá múltiples dominios de difusión.

A continuación se enumeran ciertas razones por las que una compañía quisiera implementar VLANs:

- ***Reducción del Coste de Movimientos y Cambios:*** Porque resulta más conveniente y económica la administración de redes dinámicas, lo que se traduce en ahorro de tiempo y dinero.
- ***Seguridad:*** Porque se restringen las probabilidades de que las personas no autorizadas tengan acceso a la información de la red. Además el único tráfico de información en un segmento de un sólo usuario será de la VLAN de ese usuario, por lo que sería imposible "escuchar" la información si no nos es permitida, incluso poniendo el adaptador de la red en modo promiscuó, porque ese tráfico de información no pasa físicamente por ese segmento.

- ***Aplicaciones y Proyectos Especiales:*** Porque se simplifica el trabajo en una aplicación especializada al tiempo que se agrupan todos los nodos involucrados en el proyecto.
- ***Desempeño y Ancho de Banda:*** El ancho de banda se mejora, porque al segmentar la red por VLANs, separo los dominios de difusión, por ende "tengo control" sobre las difusiones y no permito que se difundan en toda la red.
- ***Flujo de Difusión y Tráfico:*** Porque se reducen automáticamente las difusiones, debido a que el tráfico de difusión no pasa a nodos que no hagan parte de la VLAN especifica, ya que las listas de control de acceso proveen al administrador de una forma de control de quién ve cuál tráfico de red.
- ***Tareas Departamentales y Específicas:*** Porque se requiere separar a los usuarios "pesados" de la red (tales como multimedios e ingeniería), o definir perfiles especiales entre departamentos que estén dedicados a empleados importantes que necesitan tener una visión global de la organización (tales como gerentes o directores de proyecto).
- ***La Velocidad de la Red:*** Porque con la implementación de las VLAN se optimiza la gestión de puertos.
- ***Grupos de Trabajo Virtuales:*** Porque a través de todo el entorno de red del campus, miembros del mismo departamento o sección puedan simular el compartir la misma red local, sin que la mayoría del tráfico de la red esté en el mismo dominio de *broadcast* de la VLAN. Alguien que se mueva a una nueva localización física pero que permanezca en el mismo departamento se podría mover sin tener que reconfigurar la estación de trabajo. Lo que ofrece un entorno más dinámicamente organizado, permitiendo la tendencia hacia equipos con funciones cruzadas.

3. ENLACE TRONCAL DE VLANS (TRUNKING):

3.1. Historia:

Los antecedentes del enlace troncal provienen directamente de los orígenes de las tecnologías radiales y telefónicas. Haciendo una semejanza entre ambas tecnologías, podríamos decir que a nivel radial un enlace troncal es una sola línea de comunicación que transporta múltiples canales de señales de radio y que a nivel de conmutación *"un enlace troncal es una conexión física y lógica entre dos switches a través de la cual viaja el tráfico de red"*[7]

3.2. Definición:

"En una red conmutada, un enlace troncal es un enlace punto a punto que admite varias VLANs, el propósito de un enlace troncal es conservar los puertos cuando se crea un enlace entre dos dispositivos que implementan las VLANs, el enlace troncal agrupa múltiples enlaces virtuales en un enlace físico, esto permite que el tráfico de varias VLANs viaje a través de un solo cable entre los switches"[8]

3.3. Protocolos y Mecanismos:

Los protocolos de enlace troncal fueron diseñados para gestionar la transferencia de tramas de diferentes VLANs a través de sola línea de conexión de manera efectiva. Los protocolos de enlace troncal acuerdan la forma en que se realizará la distribución de tramas a los puertos asociados en ambos extremos del enlace, ya que es el único enlace físico entre dos switches que puede transportar tráfico para cualquier VLAN, a través de la rotulación de cada trama para identificar a qué VLAN pertenece. Cabe resaltar que el enlace troncal como tal, no pertenece a ninguna VLAN en particular, sino que es un conducto de comunicación.

Existen dos mecanismos de enlace troncal, pero solo uno fue apadrinado por la IEEE como estándar y fue el Etiquetado de Tramas, ya que es muy rápido y fácil de administrar, aunque el Filtrado de Tramas también es muy utilizado.

Así mismo, existen dos esquemas de etiquetado de tramas para los segmentos Ethernet que son:

---

[7] Semestre 3 CNNA, Modulo 9: Protocolos de enlace troncal de VLAN extraído de http://serapa.blogspot.com/2008/01/mdulo-9-protocolos-de-enlace-troncal-de.html

[8] Conceptos de enlace troncal extraído de http://www.trokotech.com/manuales/cisco/ccna_v3_esp/sem3/CHAPID=knetAYhFIplFBgMCMVMA/RLOID=knet-AYhFIpllAgKXAQUA/RIOID=knet-AUkBQIKFAAgwcjRQ/knet/AYhFIplFBgMCMVMA/content.html

- ISL – Un protocolo propietario de Cisco.
- 802.1Q – Un estándar IEEE.

El etiquetado de trama de VLANs se ha diseñado específicamente para las comunicaciones conmutadas y funciona de la siguiente manera, se coloca un identificador único en el encabezado de cada trama y a medida que se envía por todo el backbone de la red, cada switch de la red esta en la capacidad de examinar la trama antes de enviar el mensaje a otros switches, equipos terminales (el switch eliminaría el identificador) o mensajes de difusión. Este esquema funciona a nivel de Capa 2 y no necesita de muchos recursos para su gestión

Cisco como parte de sus soluciones de redes elaboró el protocolo de enlace troncal de VLANs (VTP) para resolver problemas operacionales presentes en las redes conmutadas generados a partir del crecimiento y la complejidad estructural de la misma.

Tomemos como ejemplo un problema operacional común, causado por la asignación incorrecta de una VLAN, lo cual genera entre otros los siguientes conflictos:

- *"Conexión cruzada entre las VLANs debido a las incongruencias de la configuración de VLANs.*
- *Los errores de configuración de VLANs entre entornos de medios mixtos como, por ejemplo, Ethernet e Interfaz de Datos Distribuida por Fibra (FDDI)"*[9]

Justamente este tipo de problemas son los que pretende solucionar VTP, manteniendo unificada configurada del dominio, además de reducir la complejidad de la administración y el monitoreo de redes que tienen las VLANs.

Ahora si, procedamos a definir VTP y a describir como funciona, VTP es un protocolo de mensajes que usa tramas de enlace troncal de Capa 2 para el manejo de de las VLANs en un solo dominio, realizando cambios de manera centralizada que se propagan a todos los switches de la red.

En este protocolo los mensajes se encapsulan en las tramas del protocolo de enlace (Inter-Switch (ISL)) y se envían a través de enlaces troncales a otros dispositivos. VTP maneja un encabezado según el tipo de mensaje, pero por lo general siempre contiene los mismos elementos:

- Versión del protocolo.
- Tipo de mensaje.
- Longitud del nombre de dominio de administración.

[9] Semestre 3 CNNA, Modulo 9: Protocolos de enlace troncal de VLAN extraído de http://serapa.blogspot.com/2008/01/mdulo-9-protocolos-de-enlace-troncal-de.html

- Nombre de dominio de administración.

"Con VTP, cada switch publica en sus puertos troncales su dominio de administración, número de revisión de configuración, las VLANs que conoce y determinados parámetros para cada VLANs conocida. Todos los dispositivos en el mismo dominio de administración reciben información acerca de cualquier nueva VLANs que se haya configurado en el dispositivo transmisor"[10].

Existen tres clases de mensajes VTP:

- Peticiones de Publicación: Solicitan información de las VLAN.
- Publicaciones de Resumen: Respuestas del servidor a las solicitudes previamente descritas.
- Publicaciones de Subconjunto: Respuestas del servidor a las solicitudes previamente descritas.

Según se amplía la cantidad de VLANs en una red, es recomendable la utilización del enlace troncal de VLAN para asignar varias VLANs a una interfaz de router única y esta es precisamente es una de las ventajas principales de este protocolo puesto que reduce la cantidad de puertos de router y switch que se utilizan, lo que se refleja no solo en ahorro de dinero, sino también reduce la complejidad de la configuración de la red .

"Las VLANs se pueden extender a múltiples switches y se puede tener más de una VLANs por switch. Para que múltiples VLANs en múltiples switches sean capaces de comunicarse usando un enlace común, se debe usar un proceso denominado trunking -- trunking es la tecnología que permite que la información de múltiples VLANs sea transportada sobre un enlace único entre switches"[11].

Tomemos como ejemplo el esquema representado en la figura 6, donde cada switch tiene dos VLANs, al primer switch pertenecen las VLANs A y B, las cuales se comunican por medio de un puerto (trunking) hacia el router con destino hacia el segundo switch, así mismo las VLANs C y son troncalizadas desde el segundo switch hacia el primero y desde el primero hacia el router y por esta troncal principal, transita todo el trafico de las cuatro VLANs y debido a la transparencia del algoritmo de puente y de troncalizado, ambos equipos y el router piensan que se encuentran en el mismo segmento físico.

[10] Implementación de VTP extraído de http://www.trokotech.com/manuales/cisco/ccna_v3_esp/sem3/CHAPID=knet-AYhFIplFBgMCMVMA/RLOID=knet-AUkBQJJnAgNokyVw/RIOID=knet-AUkBQAMEAwkhSDFg/knet/AYhFIplFBgMCMVMA/content.html

[11] VLANs, para qué son y para qué sirve, extraído de http://www.fedora-ve.org/content/view/54/52/

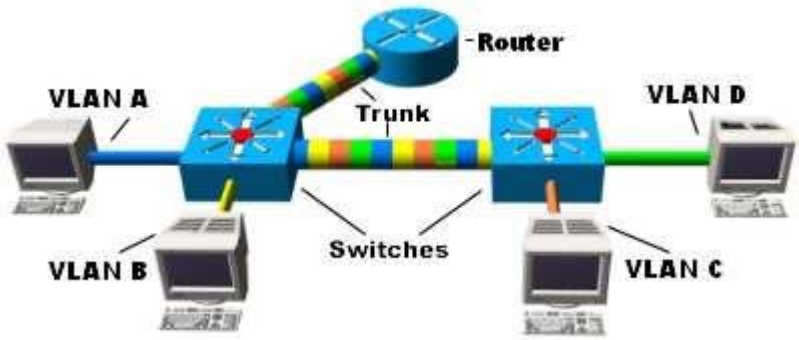

Figura 9. Trunking.

Fuente: http://www.fedora-ve.org/content/view/54/52/.

4. ACLS (Listas de Acceso):

4.1. Generalidades:

Desde los inicios de los sistemas computacionales siempre ha existido la necesidad de restringir el acceso a determinadas partes de la red y mayormente aun a redes externas e Internet, por motivos de seguridad, privacidad, protección de la información, entre otros. Esta necesidad comenzó a saciarse con la aparición de las Listas de Acceso y la utilización de las funciones de filtrado de paquetes de los software IOS, con las cuales un administrador de red puede restringir el acceso a determinados sistemas, segmentos de red, rangos de direcciones y servicios, basándose en una serie de criterios.

Funcionalmente los routers utilizan las Listas de Control de Acceso para identificar el tráfico circulante en la red, y es manejada para el filtrado del mismo, con lo que se consigue una mejor administración del tráfico global de la red, por ello, las Listas de Acceso constituyen una poderosa herramienta para el control de la red, ya que cuentan con la flexibilidad necesaria para filtrar el flujo de paquetes que entra y sale de las distintas interfaces del router, permitiendo controlar el movimiento de estos dentro de la red.

4.2. Definiciones:

"Las ACLs son listas de instrucciones que se pueden aplicar a la interfaz de un router, las sentencias se evalúan en el orden en que fueron introducidas en la ACLs y cuando llegan los paquetes se comparan uno a uno y en secuencia con instrucción por instrucción hasta encontrar una coincidencia y una vez encontrada, se ejecuta la acción especificada en la sentencia y no se comprueban más condiciones "[12].

A nivel de Seguridad podemos definir las Listas de Control de Acceso como un "concepto de seguridad informática usado para fomentar la separación de privilegios; como una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido, permitiendo controlar el flujo del tráfico en equipos de redes, tales como routers y switches"[13].

El objetivo primordial de toda lista de acceso es el filtrado de tráfico, teniendo en cuenta algunos criterios definidos previamente y como alternativa colindante la identificación de tráfico "interesante", es decir, aquel suficientemente importante para activar o mantener una conexión en una ISDN (Red digital de Servicios Integrados).

---

[12] ACL Listas de Control de Acceso extraído de http://www.arud.uji.es/dicc-wiki/index.php?title=ACL_Listas_de_Control_de_Acceso

[13] Lista de Control de Acceso extraído de http://buenmaster.com/?a=537

A nivel de Redes podemos indicar que las ACLs se refieren a una lista de políticas que describen puertos de servicio o nombres de dominios disponibles en una terminal o dispositivo de capa de red, cada uno de ellos con una lista de terminales y/o redes que tienen consentimiento para usar el servicio.

Características:

- Una ACL se aplica a una interfaz ya sea de entrada o de salida.
- Se puede crear una ACL para la interfaz de salida y otra para la interfaz de entrada.
- Las ACLs son sucesiones de instrucciones que son verificadas contra el paquete.
- El orden de las instrucciones es importante, ya que cuando una línea de la secuencia es verdadera en la verificación, se toma una acción y se sale de la ACL, es decir no se continúa verificando para comprobar que haya otra línea de la secuencia que también resulte cierta.
- No se pueden insertar líneas que por error no fueron incluidas en la secuencia, puesto que si lo queremos hacer, figuraría borrar TODA la ACL y volverla a crear.
- La última línea de una lista de acceso NUNCA aparece, es decir existe de forma explicita y siempre es DENIEGO TODO.

4.4. Funcionalidades:

Las Listas de Acceso (ACLs) se aplican para el filtrado de paquetes en base a ciertos parámetros, entre los cuales encontramos: las direcciones de red origen o destino, los puertos origen o destino y el tipo de protocolo.

La principal aplicación de las Listas de Acceso es a nivel de Seguridad de Redes, ya que con ellas se puede restringir e inclusive bloquear el tráfico no deseado en una interfaz de entra o salida. No obstante, existen otras aplicaciones relacionadas con el filtrado de rutas al crear políticas de encaminamiento.

Técnicamente las ACLs comprendidas entre 1 y 199 se utilizan en TCP/IP, mientras que las comprendidas entre 800 y 999 se utilizan para IPX/SPX, el resto de rango rangos se utilizan para DECnet (300-399), XNS (400-599), AppleTalk (600-699), en todo caso al entra en materia con los tipos de ACLs veremos este tema a mayor profundidad.

4.5. Tipos de ACLs y Comandos:

4.5.1. ACLs Estándar: *"Una ACL* estándar *consiste exclusivamente en las entradas de tipo* owner *(propietario),* owning group *(grupo propietario) y* other *(otros) y coincide con los bits de permisos tradicionales para archivos y directorios".*[14]. Se especifica solo una dirección de origen; y se permite o deniega el acceso a un conjunto de protocolos. La numeración para las ACLs Estándar esta comprendida entre 1 y 99 o entre 1300 y 1999.

Comando: access-list ACL# {deny|permit} {@IPsource WildcardMásk | host @IPsource | any} ip access-group ACL# {in |out}.

El primer comando, access-list, crea la lista de acceso con número ACL# y con la condición deniego o permito el acceso sobre la dirección IP origen especificada con la correspondiente wildcard mask.

El segundo comando, access-group, asigna la lista de acceso ACL# sobre la interfaz de entrada o de salida donde se ejecuta dicho comando.

Ejemplo: Deneguemos en la interfaz s0 de salida cualquier paquete IP que provenga de la red 10.1.1.0/24.

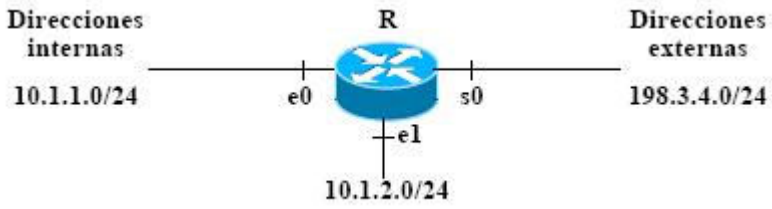

Figura 10. Denegación de Servicio en una ACL Estándar.

Fuente: personals.ac.upc.edu/jo**se**b/XC-Lab-5-**ACL**s.pdf

```
R# configure terminal
R(config)# access-list 1 deny 10.1.1.0 0.0.0.255
R(config)# access-list 1 permit any
R(config)# interface s0
R(config-if)# ip access-group 1 out
R(config-if)# exit
R# show access-lists
```

[14] Funcionamiento de las ACLs extraído de http://www.l3jane.net/doc/linux/suse/suselinux-adminguide_es/apbs03.html#tab:entrytype

Primeramente se crea acceso, seguidamente se deniega todo tráfico que venga de la red 10.1.1.0/24, pero como la última línea deniega implícitamente todo lo demás (e.g.; la red 10.1.2.0/24), previamente se permite el acceso del resto de las direcciones; esta ACL es aplicada sobre la interfaz de salida s0.

4.5.2. ACLs Extendida: *"Una ACL* extendida *(extended) contiene además una entrada* mask *(máscara) y puede incluir varias entradas del tipo* named user *(usuario identificado por el nombre) y* named group *(grupo identificado por el nombre)*[15]*.* En su sintaxis encontramos el protocolo y una dirección de origen y de destino, permitiendo mayor flexibilidad y control, en la medida que comprueban direcciones IP de origen y destino y también comprueban protocolos y l números de puerto TCP y UDP. La numeración para las ACLs Extendidas esta comprendida entre 100 y 199 o entre 2000 y 2699.

Comando: access-list ACL# {deny|permit} protocol {@IPsource WildcardMásk | host @IPsource| any} {@IPdest WildcardMásk | host @IPdest | any} {operador port} ip access-group ACL# {in |out}.

El primer comando, access-list, crea la lista de acceso con número ACL# y con la condición deniego o permito el acceso sobre la dirección IP origen y/o destino especificadas con las correspondientes wildcard masks.

Ejemplo: Deneguemos en la interfaz s0 de salida cualquier paquete ICMP que provenga de la red 10.1.1.0/24 y el acceso a cualquier puerto telnet por parte de un host de esa red.

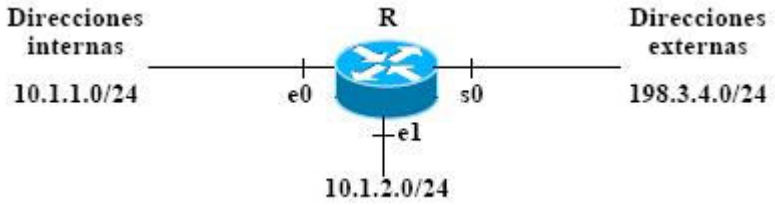

Figura 11. Denegación de Servicio en una ACL Extendida.

Fuente: personals.ac.upc.edu/jo**se**b/XC-Lab-5-**ACL**s.pdf

[15] Funcionamiento de las ACLs extraído de http://www.l3jane.net/doc/linux/suse/suselinux-adminguide_es/apbs03.html#tab:entrytype

```
R# configure terminal
R(config)# access-list 101 deny icmp 10.1.1.0 0.0.0.255 any
R(config)# access-list 101 deny tcp 10.1.1.0 0.0.0.255 any eq 23
R(config)# access-list 101 permit any any
R(config)# interface s0
R(config-if)# ip access-group 101 out
R(config-if)# exit
R# show access-lists
```

Primeramente creamos la lista de acceso extendida, seguidamente se deniega el acceso de paquetes ICMP, posteriormente se deniega el acceso a cualquier host con puerto 23, y finalmente se permite cualquier otro tipo de tráfico y a continuación se aplica la lista de acceso a la interfaz de salida s0.

4.5.3. ACLs Nombradas: Una ACL *nombrada* permite asignar nombres a las ACLs estándar y extendida, mejorando su identificación, eliminando los límites de la numeración de 99 para sencillas y 100 de extendidas, y permitiendo modificar las ACLs sin tener que borrarlas y después reconfigurarlas.

4.6. Razones y Recomendaciones de Uso:

Razones de Uso:

- Limitar el tráfico de red y mejorar el rendimiento de la misma.
- Brindar control de flujo de tráfico.
- Proporcionar un nivel básico de seguridad para el acceso a la red.

Recomendaciones de Uso:

- Una ACLs por interfaz.
- Sólo se pueden borrar ACLs completas.
- Las ACLs no filtras tráfico originado en el mismo router.
- Si no hay coincidencias con ninguna regla existe una denegación implícita.
- Las ACLs salientes son más eficaces al comprobar menos paquetes.

4.7. Wildcard Mask:

Puede ser necesario corroborar condiciones para un grupo o rango de direcciones IP, o bien para una dirección IP individual y esta comprobación de direcciones tiene lugar utilizando máscaras que actúan a modo de comodines en las direcciones de la lista de acceso, para identificar los bits de la dirección IP que han de

coincidir explícitamente y cuales pueden ser ignorados. El enmascaramiento wildcard para los bits de direcciones IP utiliza los números 1 y 0 para referirse a los bits de la dirección.

La Wildcard Mask es una máscara de 32 bits que indica que bits de la dirección IP se tienen que comprobar y cuales no; un bit de máscara wildcard 0 significa “comprobar el valor correspondiente”, mientras un bit de máscara wildcard 1 significa “Ignorar el valor del bit correspondiente”.

Muy comúnmente se utilizan abreviaturas para los enmascaramientos, tales como: **Host** = máscara comodín 0.0.0.0, utilizada para un host especifico **Any** = 0.0.0.0 255.255.255.255, utilizado para definir a cualquier host, red o subred. En el caso de permitir o denegar redes o subredes completas, se deben ignorar todos los host pertenecientes a dicha dirección de red o subred y cualquier dirección de host será leída como dirección de red o subred.

Por ejemplo, deseamos corroborar que un paquete que ingresa a la red pertenezca al host con dirección IP 145.34.5.6, por lo tanto verificaremos todos los bits de la dirección IP, lo que significa que la wildcardmásk sería 0.0.0.0.

5. SEGURIDAD PERIMETRAL:

5.1. Historia:

En la historia de la Seguridad Informática una de sus principales inquietudes ha sido salvaguardar el perímetro, porque si se logra proteger esta parte de la red, el administrador de la misma, tendrá la confianza de que la red interna esta segura; hoy día esta seguridad perimetral se logra con la adaptación de un firewall en el borde de la red.

Antiguamente en el perímetro de una red organizacional, solo estaban definidos y dentro del mismo segmento físico y lógico servidores y equipos de trabajo y existía un único enlace dedicado a Internet, pero hoy por hoy la situación de las redes corporativa es otra, se cuenta con más de un enlace hacia Internet (redundancia), con redes inalámbricas, VPN, WAN y lógicamente con los servidores y los equipos de trabajo.

Por todos esto motivos, la Seguridad de la Información es ahora más compleja, las amenazas y vulnerabilidades siguen existiendo, aunque de forma diferente y la tecnología avanza en pro de desarrollar sistemas más seguros, por lo que se han creado una inanidad de soluciones tales como: Firewalls corporativos con opción de VPN, Antivirus para servidores y estaciones de trabajo, Detectores de intrusos reactivos a nivel de host y red, entre otras muchas tantas. Pero a pesar de que la tecnología existe, el principal problema en nuestros días es saber utilizar estos recursos de forma tal que se pueda tener un control total sobre lo que existe en la red, mantener la visibilidad de lo que está ocurriendo y corroborar que lo que se hace está dentro del marco de políticas aceptadas por la organización.

La seguridad hoy día es convergente y se implementa por aproximación por capas, como lo podemos observar en la siguiente imagen, puesto que la seguridad es un proceso continuo y no un producto, es una mezcla de soluciones y practicas que se extiende a los elementos de la red y surge de la cooperación y compenetración de los mismos con la Infraestructura Tecnológica.

Figura 12. Seguridad Convergente y Aproximación por Capas.

Fuente: Maldonado, Pablo. Tendencias en Seguridad para ecosistemas IP en redes convergentes fijo-móviles. Congreso internacional telefonía IP. Monterrey 2006 Alcatel.

5.2. Generalidades:

Los problemas de seguridad en una red organizacional, comienzan en el preciso momento en que los equipos de trabajo se conectan a Internet, puesto que abren una gran puerta que trae consigo toda una serie de nuevos y complejos tipos de amenazas y ataques.

"Existe un acuerdo y conciencia general sobre la importancia de la Seguridad de los Sistemas de Información (denominado SSI). La SSI está relacionada con la disponibilidad, confidencialidad e integridad de la información tratada por las computadoras y las redes de comunicación"[16].

5.3. Definición:

Se define como Seguridad Perimetral el correcto uso y configuración de los equipos de seguridad y protección que controlan y resguardan el tráfico y contenido de entrada y salida entre todos los puntos de conexión entre si mismos y con el perímetro de la red, acompañado de una correcta implementación de las políticas de seguridad.

5.4. Acciones para mejor la Seguridad en la LAN:

- *"Implementar políticas de navegación más complejas y robustas a nivel de Firewall de Software que se integre al controlador de*

[16] http://itcp-cerbesa.blogspot.com/2006/10/seguridad-it-parte-1-aspectos-para.html

dominio para restringir el acceso a páginas o recursos de Internet por IP y usuario y al mismo tiempo optimizar el uso del ancho de banda contratado del enlace y optimizar el tiempo de los empleados. Esta tarea también se puede implementar a través de la soluciones de Web Security que permite realizar filtros de navegación a nivel de usuario de dominio.

- *Actualizar los parches de seguridad y vulnerabilidades de todos los servidores de la organización y las estaciones de trabajo. Al mantener actualizados los sistemas operativos de las máquinas críticas se reduce el riesgo de que se filtre un ataque diseñado a propagarse aprovechando alguna vulnerabilidad del sistema operativo. Esto se puede realizar a través de la herramienta de Microsoft Software Update Services (SUS).*
- *Utilizar la herramienta de Microsoft Baseline Security Analyzer antes y después de aplicar parches a través de Windows Update. Al ejecutar esta herramienta reporta los parches que aun no han sido aplicados en una forma más eficiente así se puede tomar una acción preventiva.*
- *Se recomienda que internamente se haga un piloto de cada uno de las soluciones seguridad (Antivirus) y validar cual da mayores beneficios a la organización con el objetivo de estandarizar a una sola herramienta.*
- *Se recomienda montar una solución en el Servidor de correo que monitoree los buzones de los usuarios para spam y antivirus que se podrían estar enviando internamente.*
- *Implementar una solución de IDS con sus respectivas bitácoras para poder tener certeza de que es esta sucediendo en al red LAN. Implementar una solución IPS para que al momento de que el IDS detecte el ataque, el IPS lo bloquee inmediatamente.*
- *Implementar herramientas anti Spam.*
- *Implementar herramientas anti Adware, Spyware, Phishing, etc."*[17]

5.5. Seguridad de Perímetro Organizacional WAN e Internet:

Como lo mencionábamos con anterioridad, la salida a Internet es una gran puerta abierta para la inseguridad de nuestra red, y mucho más aun hoy día cunado mayor parte de los ataques son perpetrados desde exterior de nuestra red. En esta medida, lo primero que hay que garantizar es que los usuarios que están pretendiendo acceder a la red sean los usuarios autorizados, y que cuentan con el certificado de autenticidad del caso.

Con relación a los accesos del Internet es importante que la empresa posea un FIREWALL que sea capaz de hacer las funciones de:

- Antivirus.

[17] http://itcp-cerbesa.blogspot.com/2006/10/seguridad-it-parte-3-auditora-de-los.html

- IDS.
- IPS.
- Filtrado de Contenido.
- Anti Spam.
- Inspección total de paquetes en transito.

Con un dispositivo de seguridad de estas magnitudes y sumándole el hecho de desactivar todos los modem que existan en los equipos de trabajo o servidores, se evitarán agujeros de seguridad en la puerta principal y puertas trasera respectivamente.

Es recomendable que la autenticación de los usuarios cumpla un mínimo de tres métodos de autenticación:

- Usuario registrado para acceder a la aplicación o recurso.
- Password de usuarios, con características de complejidad alta, o sea que lleve letras, símbolos y números en el password como tal.
- Llave física o Token que contengan el certificado emitido por el controlador de dominio, el cual valida y verifica al usuario.

Sin embargo, todo el proceso relacionado con Seguridad Informática se basa en tres pilares fundamentales que se detallaran a continuación, los cuales intercambian su orden de prioridad dependiendo del tipo de de sistema informático.

5.5.1. Pilares de la Seguridad Informática:

5.5.1.1. Confidencialidad: "*La confidencialidad, a veces denominada secreto o privacidad, se refiere a la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él*"[18]

En términos generales, la confidencialidad asegura que los usuarios puedan acceder a la información que les está permitida de acuerdo a disposiciones organizacionales, estratégicas o legales.

Algunos de los mecanismos utilizados para salvaguardar la confidencialidad de los datos son, por ejemplo:

- El uso de técnicas de control de acceso a los sistemas.
- El cifrado de la información confidencial o de las comunicaciones.

[18] Seguridad Informática extraído de http://www.lasalle.edu.co/csi_cursos/informatica/termino/seguridad_informatica.htm

5.5.1.2. Integridad: Es el servicio de seguridad que certifica que la información solamente sea creada, modificada o borrada por los usuarios autorizados para dicho fin, porque de lo contrario se corrompe la información perdiendo credibilidad e inclusive su valor económico. Vale la pena resaltar que este aspecto, no solo se tiene en cuenta las modificaciones causadas de manera intencional, sino también cambios realizados de manera accidental o no intencionados.

De la mano con el campo de la criptografía, se han desarrollado diferentes métodos para certificar la autenticidad de los mensajes y la precisión de los datos recibidos, entre ellos encontramos: códigos/firmas añadidos a los mensajes en origen y recalculadas/comprobadas en el destino.

5.5.1.3. Disponibilidad: "*Se entiende por disponibilidad el grado en que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado; o la situación que se produce cuando se puede acceder a un SSI en un periodo de tiempo considerado aceptable*" [19]

Para que un sistema se considere como disponible, deberá cumplir dos requisitos fundamentales: lo primero es que el sistema (hardware/software) se mantenga funcionando eficientemente y lo segundo que sea capaz de recuperarse rápidamente en caso de fallo.

5.5.2. Aspectos relevantes para la Seguridad:

Existen otros aspectos importantes que van de la mano con los pilares básicos de la Seguridad Informática y que actúan como complementos de los mismos, ellos son:

5.5.2.1. Autenticidad: Este aspecto permite validar y asegurar el origen de la información, de modo tal que se puede demostrar que es quien dice ser.

5.5.2.2. Imposibilidad de Rechazo (No Repudio): Este aspecto permite certificar que cualquier entidad que envía o recibe información, no puede fundamentar ante terceros que no la envió o la recibió.

5.5.2.3. Consistencia: Este aspecto asegura que el sistema se comporte como se presume que debe hacerlo con los usuarios que debe hacerlo (autorizados).

[19] Estándares de la Informática: Información y sistema Informático extraído de http://itcp-cerbesa.blogspot.com/2006/10/estndares-de-la-informtica.html

5.5.2.4. Aislamiento: Este aspecto regula el acceso al sistema, impidiendo que personas no autorizadas entren en él.

5.5.2.5. Política de Seguridad: *"La política de seguridad es una declaración de intenciones de alto nivel que cubre la seguridad de los SSI y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán. La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las distintas medidas a tomar para proteger la seguridad del sistema, las funciones y responsabilidades de los distintos componentes de la organización y los mecanismos para controlar su correcto funcionamiento"* [20]. Estas políticas deberán ser de tres tipos:

- Laborales.
- Hardware.
- Software.

5.5.3. Vulnerabilidades, Amenazas y Contramedidas:

5.5.3.1. Vulnerabilidad: Punto del sistema que es susceptible de ser atacado, dañando la seguridad del mismo y representan las debilidades o aspectos atacables en el sistema informático.

Tipos de Vulnerabilidades:

- **Vulnerabilidad Física:** Se relaciona con la posibilidad de atentar físicamente contra el sistema, en esta categoría se incluyen también los robos.
- **Vulnerabilidad Natural:** Se relaciona con las condiciones geográficas, geológicas, marítimas y atmosféricas que pueden afectar el sistema tras alguna catástrofe natural o por factores como el polvo, la humedad, el calor, etc.
- .**Vulnerabilidad del Hardware y/o Software:** Se relaciona con las susceptibilidades físicas que pueden tener o sufrir los equipos o problema a nivel de sistema operativo o software que permiten realizar ataques.
- **Vulnerabilidad de los Medio y/o Dispositivos:** Se refiere a la posibilidad de robar o dañar los discos, cintas, listados de impresora, etc.
- **Vulnerabilidad por Emanación;** Relacionados con la intercepción de las emanaciones trasmitidas por los equipos eléctrico y electrónicos que permitan la posterior reconstrucción de la información almacenada o transmitida.

[20] Estándares de la Informática: Parte 2 Políticas de Seguridad extraído de http://itcp-cerbesa.blogspot.com/2006/10/estandares-de-la-informatica-parte-2.html

- **Vulnerabilidad de las Comunicaciones:** Relacionado con el riesgo de intercepción de las comunicaciones trasmitidas en la red..
- **Vulnerabilidad Humana:** Los usuarios del sistema también suponen un gran riesgo al mismo, ya que son ellos quienes pueden acceder al medio tanto física como lógicamente**.**

5.5.3.2. Amenaza: Posible peligro del sistema, que puede ser una persona (cracker), un programa (virus, caballo de Troya, etc.), o un suceso natural o de otra índole (fuego, inundación, etc.), aprovechándose de las debilidades del sistema.

Tipos de Amenazas:

- **Intercepción:** Cuando una persona, programa o proceso logra el acceso a una parte del sistema a la que no está autorizada.
  Ejemplos:
  - Escucha de una línea de datos.
  - Copias de programas o ficheros de datos no autorizados.

  Son los más difíciles de detectar pues en la mayoría de los casos no alteran la información o el sistema.

- **Modificación:** Se trata no sólo de acceder a una parte del sistema a la que no se tiene autorización, sino, además, de cambiar en todo o en parte su contenido o modo de funcionamiento.
  Ejemplos:
  - Cambiar el contenido de una base de datos.
  - Cambiar líneas de código en un programa.
  - Cambiar datos en una transferencia bancaria.

- **Interrupción:** Interrumpir mediante algún método el funcionamiento del sistema.
  Ejemplos:
  - Saturar la memoria o el máximo de procesos en el sistema operativo.
  - Destruir algún dispositivo hardware.

- **Generación:** Se refiere a la posibilidad de añadir información o programas no autorizados en el sistema.
  Ejemplos:
  - Añadir campos y registros en una base de datos.

- Añadir código en un programa (virus).
- Introducir mensajes no autorizados en una línea de datos.

- **Amenazas Naturales o Físicas:** Son las que ponen en peligro los componentes físicos del sistema. Entre ellas tenemos: desastres naturales, y condiciones medioambientales.

- **Amenazas Involuntarias:** Son aquellas relacionadas con el uso descuidado del equipo por falta de entrenamiento o de concienciación sobre la seguridad. Entre las más comunes podemos citar:

  - Borrar sin querer parte de la información.
  - Dejar sin protección determinados ficheros básicos del sistema.
  - Dejar pegado a la pantalla un post-it con nuestro password u olvidarnos de salir del sistema.

- **Amenazas Intencionadas:** Son aquellas procedentes de personas que pretenden acceder al sistema para borrar, modificar o robar la información; para bloquearlo o por simple diversión. Los causantes del daño pueden ser de dos tipos: internos y externos. Los externos pueden penetrar al sistema de múltiples formas:

  - Entrando al edificio o accediendo físicamente al ordenador.
  - Entrando al sistema a través de la red explotando las vulnerabilidades software del mismo.
  - Consiguiendo acceder a través de personas que lo tienen de modo autorizado.

5.5.3.3. Contramedidas: Técnicas de protección del sistema contra las amenazas.

Tipos de Medidas de Seguridad o Contramedidas:

Los sistemas informáticos pueden diseñarse de acuerdo con criterios de economía, de eficiencia y de eficacia, etc., porque son claramente medibles y se asocian a parámetros que, maximizando unos y minimizando otros, se puede tender hacia diseños óptimos.

Las medidas de seguridad que pueden establecerse en un sistema informático son de cuatro tipos fundamentales:

- **Medidas Físicas:** Aplican mecanismos para impedir el acceso directo o físico no autorizado al sistema. También protegen al sistema de desastres naturales o condiciones medioambientales adversas.

Existen tres factores fundamentales a considerar:

- El acceso físico al sistema por parte de personas no autorizadas.
- Los daños físicos por parte de agentes nocivos o contingencias.
- Las medidas de recuperación en caso de fallo

Concretando algo más los tipos de controles que se pueden establecer, estos incluyen:

- Control de las condiciones medioambientales (temperatura, humedad, polvo, etc.)
- Prevención de catástrofes (incendios, tormentas, cortes de fluido eléctrico, sobrecargas, etc.)
- Vigilancia (cámaras, guardias jurados, etc.)
- Sistemas de contingencia (extintores, fuentes de alimentación ininterrumpida, estabilizadores de corriente, fuentes de ventilación alternativa, etc.)
- Sistemas de recuperación (copias de seguridad, redundancia, sistemas alternativos geográficamente separados y protegidos, etc.)
- Control de la entrada y salida de material (elementos desechables, consumibles, material anticuado, etc.)

- **Medidas Lógicas:** Incluye las medidas de acceso a los recursos y a la información y al uso correcto de los mismos, así como a la distribución de las responsabilidades entre los usuarios. Se refiere más a la protección de la información almacenada.

  Entre los tipos de controles lógicos que es posible incluir en una política de seguridad podemos destacar los siguientes:

  - Establecimiento de una política de control de accesos. Incluyendo un sistema de identificación y autentificación de usuarios autorizados y un sistema de control de acceso a la información.
  - Definición de una política de instalación y copia de software.
  - Uso de la criptografía para proteger los datos y las comunicaciones.
  - Uso de cortafuegos (Firewall) para proteger una red local de Internet.
  - Definición de una política de copias de seguridad.
  - Definición de una política de monitorización (logging) y auditoria (auditing) del sistema.

Dentro de las medidas lógicas se incluyen también aquellas relativas a las personas y que podríamos denominar medidas humanas. Se trata de definir las funciones, relaciones y responsabilidades de distintos usuarios potenciales del sistema. Se trataría entonces de responder a preguntas tales como:

- ¿A quién se le permite el acceso y uso de los recursos?
- ¿Qué recursos puede acceder cada usuario y qué uso puede hacer de ellos?
- ¿Cuáles son las funciones del administrador del sistema y del administrador de la seguridad?
- ¿Cuáles son los derechos y responsabilidades de cada usuario?

A la hora de responder a las preguntas anteriores hemos de diferenciar cuatro tipos fundamentales de usuarios. A cada tipo se le aplicará una política de control de accesos distinta y se le imputaran distinto grado de responsabilidades sobre el sistema:

- El administrador del sistema y en su caso el administrador de la seguridad.
- Los usuarios del sistema.
- Las personas relacionadas con el sistema pero sin necesidad de usarlo.
- Las personas ajenas al sistema

- **Medidas Administrativas:** Las medidas administrativas son aquellas que deben ser tomada por las personas encargadas de definir la política de seguridad para ponerla en práctica, hacerla viable y vigilar su correcto funcionamiento. Algunas de las medidas administrativas fundamentales a tomar son las siguientes:

  - Documentación y publicación de la política de seguridad y de las medidas tomadas para ponerla en práctica.
  - Debe quedar claro quien fija la política de seguridad y quien la pone en práctica.
  - Establecimiento de un plan de formación del personal.

  Los usuarios deben tener los conocimientos técnicos necesarios para usar la parte del sistema que les corresponda. Este tipo de conocimiento es fundamental para evitar toda una serie de fallos involuntarios que pueden provocar graves problemas de seguridad.

  Los usuarios deben ser conscientes de los problemas de seguridad de la información a la que tienen acceso.

Los usuarios deben conocer la política de seguridad de la empresa y las medidas de seguridad tomadas para ponerla en práctica. Además deben colaborar, a ser posible voluntariamente, en la aplicación de las medidas de seguridad.

Los usuarios deben conocer sus responsabilidades respecto al uso del sistema informático, y deben ser conscientes de las consecuencias de un mal uso del mismo.

- **Medidas Legales:** Se refiere más a la aplicación de medidas legales para disuadir al posible atacante o para aplicarle algún tipo de castigo a posteriori. Este tipo medidas trascienden el ámbito de la empresa y normalmente son fijadas por instituciones gubernamentales e incluso instituciones internacionales.

- **Planes de Contingencia:** La clave de una buena recuperación en caso de fallo es una preparación adecuada. Por recuperación entendemos tanto la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema, como la posibilidad de volver a la situación anterior al mismo habiendo reemplazado o recuperado el máximo de los recursos y de la información.

  Adicionalmente existen otros aspectos relacionados con la recuperación como son la detección del fallo, la identificación del origen del ataque y de los daños causados al sistema y la toma de medidas a posteriori contra el atacante. Todo ello se basa en buena medida en el uso de una adecuada política de monitorización y auditoria del sistema.

  La recuperación de la información se basa en el uso de una política de copias de seguridad adecuada, mientras la recuperación del funcionamiento del sistema se basa en la preparación de unos recursos alternativos.

  Una buena política de copias de seguridad debe contemplar los siguientes aspectos:

  - Qué tipos de backups se realizan: completos o incrementales.
  - Con qué frecuencia se realiza cada tipo de backup.
  - Cuántas copias se realizan y dónde se guardan.
  - Durante cuánto tiempo se guardan las copias.

5.6. Ataques de Red y VLANs:

"Básicamente los ataques de red y contra VLANs puestos en acción son posibles porque las máquinas de los atacantes se ponen en medio de

las máquinas de las víctimas, a las que hacen creer que son un elemento legítimo en la red. Como es evidente, las protecciones comunes no son suficientes para poner a salvo una red, es decir la mayoría de las empresas no tiene seguridad. David Moss planteó que las empresas están expuestas a diferentes versiones de los ataques hombre en medio, ataques remotos y locales".[21]

Entre los principales ataque tenemos: DNS Poisoning, donde el atacante cambia las entradas de DNS de un servidor público para redirigir hacia sí mismo el tráfico predestinado a otro sitio utilizando la técnica de GRE Tunneling;ARP Poisoning, que falsifica los caches ARP de las víctimas; que hace creer al switch que el atacante es la víctima; el DHCP Spoofing, que es ponerse en el lugar del DHCP de la red y pasar información falsa al blanco y que resulta en un sniffeo half-duplex porque el router mandará el paquete de regreso directamente a la víctima; el STP Mangling es ponerse como raíz (root) del árbol spanning-tree y así puede conocer el tráfico que pasa de un lado de la red a otro; el ataque ICMP Redirect manda un paquete ICMP para hacerse pasar por una gateway; otro más intenta hacerse pasar como un router con más alta prioridad y así rutear el tráfico; el ataque de ruteo envía actualizaciones de la tabla de ruteo para confundir a los equipos activos de la red.

Detallemos ahora uno de los principales ataques basados en VLANs, con el que los atacantes vulneran la seguridad de las redes virtuales.

VLAN Hopping, se maneja para atacar a una red a través el envío de paquetes a un puerto que no es habitualmente accesible y se realiza principalmente en la dinámica la dinámica del Trunking Protocolo cuando se da el proceso de negociación de la línea entre los dispositivos y el del tipo de encapsulado de telecomunicaciones.

Tipos de VLAN Hopping:

- ***Switch Spoofing:*** Si un conmutador de red esta en el lugar para autotrunking, la red atacante consigue configurar un sistema que pasa falsas o se desactiva como un interruptor. *"Esto significa que la red atacante es capaz de emular cualquiera de ISL o 802.1q señalización junto con Dynamic Trunk Protocol (DTP) de señalización"*[22]. Si tiene éxito, el hacker entra en un interruptor que da acceso a todo y que tiene una continúa necesidad de tronco. y esto permite que el sistema de ataque para obtener acceso a todas las VLANs permitido en el tronco puerto.

[21] Nortel asegura las redes extraído de http://www.esemanal.com.mx/articulos
[22] ¿Qué es la VLAN Hopping? Extraído de http://www.tech-faq.com/lang/es/vlan-hopping.shtml

- **Double Tagging:** En esta modalidad de salto de VLANs, el agresor aspira enviar datos de un cambio a otro mediante el envío de marcos con dos cabeceras 802.1Q, uno para la víctima y el otro interruptor para cambiar el ataque; la víctima acepta cambiar el marco, porque piensa que va a recibir los datos. El objetivo de cambiar el marco de lo reenvía al destino basado en el identificador de VLANs 802.1q, en la segunda cabecera.

Consecuencias del VLAN Hopping:

VLAN Hopping, puede deshabilitar cualquier medidas de seguridad pueden tener los usuarios en el lugar en el dispositivo que las rutas entre mapas de la VLANs. Hackers utilizan VLAN Hopping, para captar información sensible como detalles de la cuenta bancaria y las contraseñas de red orientada suscriptores. VLAN Hopping, también es utilizado por algunos atacantes corruptos, modificar o borrar datos del ordenador del usuario final. Otro uso de VLAN Hopping, es para propagar virus, gusanos, caballos de Troya y otros programas maliciosos, como virus y otras amenazas cibernéticas y Spyware.

Prevención del VLAN Hopping:

VLAN Hopping, puede prevenirse en cierta prorrogar por apagar el autotrunking característica de todos los interruptores que no requieren línea y siguiendo las recomendaciones concretas de cambiar de proveedor de VLANs de Seguridad.

Nunca debe usar el valor por defecto VLAN Hopping, ya sea porque es mucho más fácilmente de la VLANs por defecto. Una buena medida de seguridad es asignar todos los parámetros de las interfaces de algunas VLANs y nunca usar cualquier VLAN por defecto (normalmente VLAN 1) para nada.

CONCLUSIONES:

El trabajo que todos los días realizamos, el control que tenemos sobre nuestras finanzas, los procesos de las empresas y hasta las comunicaciones que hacen que se mueva el mundo utilizan computadoras, equipos y sistemas; es así, que se han convertido estos en algo cotidiano pero de lo cual dependemos, por eso es necesario tener todas las medidas pertinentes para evitar fallas, ataques y fraudes.

Con los procesos de reingeniería de empresas, y con las nuevas necesidades de independencia, autonomía y fluidez entre grupos de trabajo, se requieren nuevas facilidades y más dinámicas para realizar cambios en las redes.

Actualmente las VLAN combinan mayores anchos de banda, facilidades de configuración, potencial de crecimiento y manejo de seguridad en la red, lo que ayudará a que se conviertan en un Standard en los entornos corporativos.

Además las VLANs son una técnica de administración económica y sencilla para aumentar la seguridad, pues permite segmentar la red en múltiples grupos de broadcast, lo que hace posible que el administrador de red:

- Limite la cantidad de usuarios en un grupo de VLAN
- Evite que otro usuario se conecte sin recibir antes la aprobación de la aplicación de administración de red de la VLAN
- Configure todos los puertos no utilizados en una VLAN de bajo servicio por defecto.

Todas estas ventajas sugieren que este tipo de soluciones son fácilmente implementables y que además brindan a la red rendimiento, flexibilidad y seguridad.

RECOMENDACIONES:

Debido a que la información sobre las VLANs, ACLS, y Seguridad Perimetral manifiesta en esta monografía es primaria, es recomendable citar y consultar otras fuentes diferentes a las que se consultaron en este trabajo.

También se recomienda conocer al menos el funcionamiento básico de una Red de Área Local para que así se pueda entender con claridad la información descrita en el documento y poder hacer un buen uso de los conocimientos que se pueden adquirir.

Como el tema de las redes y las tecnologías es muy cambiante y a diario surgen nuevas propuestas y estándares que hacen mas robusto el funcionamiento de las mismas, se recomienda investigar constantemente y en fuentes actualizadas, con el objetivo de mejorar y actualizar el contenido presentado en esta monografía.

Se sugiere realizar un diseño de VLAN e implementarlo en laboratorios de redes donde se cuente con la infraestructura adecuada para colocar en práctica los conocimientos adquiridos a lo largo de esta investigación, y por que en entornos empresariales que así lo requieran.

No está de más recalcar que con buenas bases de conocimiento sobre el tema se pueden implementar soluciones VLAN a nivel empresarial y educativo de optimo desempeño.

GLOSARIO DE TÉRMINOS:

ACL (Access Control List): Es una lista de reglas que detallan puertos de servicio o nombres de dominios (de redes) que están disponibles en una terminal u otro dispositivo de capa de red, cada uno de ellos con una lista de terminales y/o redes que tienen permiso para usar el servicio.

APPLETALK: Es un conjunto de protocolos desarrollados por Apple Inc. para la conexión de redes. Fue incluido en un Macintosh en 1984 y actualmente está en desuso en los Macintosh en favor de las redes TCP/IP.

ATM (Asynchronous Transfer Mode): Modo de Transferencia Asíncrona, en el cual un sistema de transferencia conmuta paquetes de tamaño fijo con alta carga.

BROADCAST: Paquete de datos que se enviará a todos los nodos de una red.

DECNET: Protocolo que permitir la interconexión generalizada de diferentes computadoras principales y redes punto a punto, multipunto o conmutadas de manera tal que los usuarios puedan compartir programas, archivos de datos y dispositivos de terminal remotos.

DHCP: Protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres.

DOMINIO: Conjunto de ordenadores conectados en una red que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en dicha red.

DOWNSIZING: El concepto de "downsizing" en computación, cuya traducción más lógica podría ser la de "integración hacia micros", es la interconexión de redes de microcomputadoras con minicomputadoras y computadoras de orden principal.

DVLAN: Son puertos del switch que automáticamente determinan a que VLAN pertenece cada puesto de trabajo.

DOWNSIZING: El concepto de "downsizing" en computación, cuya traducción más lógica podría ser la de "integración hacia micros", es la interconexión de

redes de microcomputadoras con minicomputadoras y computadoras de orden principal.

ETHERNET: Tecnología desarrollada para las redes LAN que permite transmitir información entre computadoras a velocidades de 10 y 100 millones de bits por segundo.

FDDI (Fiber Distributed Data Interface): Interfaz de Datos Distribuida por Fibra para dar soporte a las estaciones de trabajo de alta velocidad, que habían llevado las capacidades de las tecnologías Ethernet y Token Ring existentes hasta el límite de sus posibilidades.

FIREWALL: Sistema que impone una política de seguridad entre la organización de red privada y el Internet, determinando cual de los servicios de red pueden ser accesados, es decir determina quien puede entrar para utilizar los recursos de red.

HUB: Concentrador que simplemente une conexiones y no altera las tramas que le llegan.

IDS: Proceso de monitorear computadoras o redes, para detectar entradas no autorizadas, actividad o modificación de archivos.

IEEE (Instituto de Ingeniería Eléctrica y Electrónica): Organización profesional entre cuyas actividades se incluye el desarrollo de estándares para comunicaciones y redes.

IP: 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.

LAN (Local Area Network): Conjunto de computadoras interconectadas entre sí, mediante un sistema de cableado o medio de comunicación, con la finalidad de compartir información y los recursos incorporados en ella.

MAC (Media Access Control): Modo de transmitir la trama por el hilo físico, que maneja el direccionamiento físico asociado a cada dispositivo, definiendo la topología de la red y la disciplina de la línea.

MAN (Metropolitan Area Network): Red de alta velocidad que cubre un área geográfica extensa. Es una evolución del concepto de LAN (red de área local),

pues involucra un área mucho más grande como puede ser una área metropolitana.

NETBIOS: Interfaz entre aplicaciones que fue desarrollada por IBM para acceder a los recursos de redes locales.

NIC (Network Interface Controller): Controlador de Interfaz de Red que es una tarjeta de expansión que permite a una DTE (Data Terminal Equipment) ordenador o impresora acceder a una red y compartir recursos entre dos o más equipos (discos duros, cdrom, etc).

REINGENIERÍA: Proceso de examinar sistemas de software existentes y/o modificarlos con ayuda de herramientas de forma automática o semi-automática.

ROUTER: Dispositivo que va directamente conectado al hub o concentrador de la Red Ethernet mediante una conexión RJ45 y que incorpora un adaptador RDSI o ADSL.

SWITCH: Dispositivo de la subred cuyo, su trabajo consiste en crear circuitos virtuales o enlazar circuitos permanentes para transmitir un flujo de información más o menos constante.

TOKEN RING: Implementación del Standard IEEE 802.5, en el cual se distingue más por su método de transmitir la información que por la forma en que se conectan las computadoras.

VLAN: Grupo de dispositivos en una o más LANs que son configurados (utilizando software de administración) de tal manera que se pueden comunicar como si ellos estuvieran conectados al mismo cable, cuando en realidad están localizados en un segmento diferente de LAN.

VTP (VLAN Trunking Protocol): Protocolo usado para configurar y administrar VLANs en equipos Cisco. VTP opera en 3 modos distintos: - Cliente - Servidor – Transparente

WAN (Wide Area Network): Tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, dando el servicio a un país o un continente

WILDCARD MASK: Mascara de 32 bits que indica que bits de la dirección IP se tienen que comprobar y cuales no. Si los bits de la máscara están a 0 entonces se comprueban, si están a 1 entonces no se comprueban.

BIBLIOGRAFÍA:

- HUIDOBRO MOYA JOSÉ MANUEL, Redes de Área Local: Informática: Administración de Sistemas Informáticos. Segunda Edición. Editorial HOMSON. Junio de 2005. Pags. 180.

- W. LELAND, M. TAQQU, W. WILLINGER, D. WILSON, "On the self-similar nature of Ethernet traffic", IEEE/ACM Trans. on Networking, Febrero 1994.

- BARLET-ROS, P.; SOLE-PARETA, J; DOMINGO-PASCUAL, J. SMARTXAC: "Sistema de monitorización y análisis de tráfico para la Anella Científica". "Boletín "Boletín de RedIRIS". (66-67): 27-30, 2004 (http://www.rediris.es/rediris/boletin/66-67/ponencia6.pdf.

- VLAN: Red de Área Local Virtual, extraído de http://www.enterate.unam.mx/Articulos/2004/noviembre/vlan.htm

- Redes Virtuales: El primer paso hacia la ubicuidad geográfica, extraído de http://www.consulintel.es/Html/Tutoriales/Articulos/vlan.html

- Redes Virtuales VLANs extraído de http://www.textoscientificos.com/redes/redes-virtuales

- Clasificación de las VLAN extraído de http://esi-10-edu.shinranet.com/web_03/clasificacion.htm

- Redes Virtuales: el primer paso hacia la ubicuidad geográfica extraído de http://www.consulintel.es/Html/Tutoriales/Articulos/vlan.html

- Semestre 3 CNNA, Modulo 9: Protocolos de enlace troncal de VLAN extraído de http://serapa.blogspot.com/2008/01/mdulo-9-protocolos-de-enlace-troncal-de.html

- Conceptos de enlace troncal extraído de http://www.trokotech.com/manuales/cisco/ccna_v3_esp/sem3/CHAPID=knet AYhFIplFBgMCMVMA/RLOID=knet-AYhFIpllAgKXAQUA/RIOID=knet-AUkBQIKFAAgwcjRQ/knet/AYhFIplFBgMCMVMA/content.html

- Semestre 3 CNNA, Modulo 9: Protocolos de enlace troncal de VLAN extraído de http://serapa.blogspot.com/2008/01/mdulo-9-protocolos-de-enlace-troncal-de.html

- Implementación de VTP extraído de http://www.trokotech.com/manuales/cisco/ccna_v3_esp/sem3/CHAPID=knet-AYhFIpIFBgMCMVMA/RLOID=knet-AUkBQJJnAgNokyVw/RIOID=knet-AUkBQAMEAwkhSDFg/knet/AYhFIpIFBgMCMVMA/content.html

- VLANs, para qué son y para qué sirve, extraído de http://www.fedora-ve.org/content/view/54/52/

- ACL Listas de Control de Acceso extraído de http://www.arud.uji.es/dicc-wiki/index.php?title=ACL_Listas_de_Control_de_Acceso

- Lista de Control de Acceso extraído de http://buenmaster.com/?a=537

- Funcionamiento de las ACLs extraído de http://www.l3jane.net/doc/linux/suse/suselinux-adminguide_es/apbs03.html#tab:entrytype

- Funcionamiento de las ACLs extraído de http://www.l3jane.net/doc/linux/suse/suselinux-adminguide_es/apbs03.html#tab:entrytype

- Seguridad Informática extraído de http://www.lasalle.edu.co/csi_cursos/informatica/termino/seguridad_informatica.htm

- Estándares de la Informática: Información y sistema Informático extraído de http://itcp-cerbesa.blogspot.com/2006/10/estndares-de-la-informtica.html

- Nortel asegura las redes extraído de http://www.esemanal.com.mx/articulos

- ¿Qué es la VLAN Hopping? Extraído de http://www.tech-faq.com/lang/es/vlan-hopping.shtml