UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERÍA

ESCUELA DE COMPUTACIÓN

TESIS DE GRADUACIÓN

PARA OPTAR POR EL TÍTULO DE

INGENIERO EN CIENCIAS DE LA COMPUTACIÓN

"DESARROLLO DE UN SERVIDOR DE ADMINISTRACIÓN DE POLÍTICAS PARA VLANS (VMPS)"

PRESENTADO POR:

SCOTT BAXTER GIAMMATEI

JOSÉ ROLANDO LIZAMA MORÁN

ASESOR:

ING. CARLOS BRAN

SEPTIEMBRE 2005

EL SALVADOR CENTROAMÉRICA

UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERÍA

ESCUELA DE COMPUTACION

COMITÉ EVALUADOR DEL TRABAJO DE GRADUACIÓN

ING. CARLOS GUILLERMO BRAN
ASESOR

ING. RAFAEL CRISTOBAL HERNÁNDEZ
JURADO

ING. CARLOS LÓPEZ LINAREZ
JURADO

ING. CARLOS ARTIGA S.
JURADO

DEDICATORIA

Quisiera agradecer a Dios por haberme dado fuerza y ser la luz de esperanza que iluminó mi camino para culminar mis estudios universitarios.

A mis padres y hermano, por apoyarme y brindarme la confianza en todo momento a lo largo de estos años.

A Paty por haber sido mi bastión de apoyo en todo este gran trayecto, porque siempre has estado a mi lado entregándome tu amor, paciencia y comprensión.

A Leonorcita por su amor incondicional y cariño que siempre me ha brindado en todo momento.

A mi tio Miguelangel por ser un gran apoyo, siempre aconsejándome para ser una mejor persona.

A mis amigos y familia que siempre han estado pendiente de lo que me ha acontecido para celebrar mis logros y ayudarme en mis fracasos.

Scott Baxter Giammatei.

DEDICATORIA

Doy gracias a Dios por darme la fortaleza y la sabiduría necesaria para culminar esta etapa de mi vida. Sin tí no soy nada Señor, gracias por todo tu amor, tu has sido mi inspiración.

A mi esposa por compartir este esfuerzo y estar siempre cerca de mí. Te amo, gracias por tu apoyo incondicional y por tu comprensión, eres lo más especial en mi vida.

A mi madre por su apoyo y consejos, porque siempre estuviste pendiente y en los momentos difíciles estuviste para apoyarme. A mi padre por la mejor herencia que me pudo dar, la educación.

Finalmente, a todos mis compañeros con los que pase desvelos, alegrías y desilusiones, con quienes aprendí a darle valor a la amistad.

Gracias,

José Rolando Lizama Morán

INDICE

CAPITULO I

1. LAS REDES VIRTUALES DE ÁREA LOCAL (VLANS)

1.1. Introducción

En el presente capítulo, se explica en que consisten las VLANs, los tipos que existen y se da algunas recomendaciones que se deben tomar en cuenta cuando se diseña redes con VLANs. También, se habla de los dispositivos de red y del funcionamiento de la red cuando estos están configurados para trabajar con VLANs. Además, se explora el tema de la implementación de VLANs en redes inalámbricas, que pueden servir para comunicar dispositivos personales como Palms, Pocket PC's, laptops con tarjetas inalámbricas, etc.

Con este capítulo, se pretende dejar en claro lo que son las VLANs y la importancia de su implementación en las redes, para que se logre comprender el motivo de esta tesis.

1.2. Definición de VLAN

Una VLAN es una red conmutada que está lógicamente segmentada en base a agrupaciones designadas por los diseñadores de la red. Estas agrupaciones pueden basarse en funciones laborales, equipos de proyectos y departamentos organizacionales entre algunas, sin importar la localización física de los equipos informáticos o de las conexiones a la red.

En otras palabras, una VLAN es un grupo de hosts con requerimientos en común que se comunican como si estuviesen conectados al mismo medio, sin interesar su localización física. La VLAN tiene los mismos atributos de una LAN física, pero permite que dispositivos se agrupen aunque no compartan el mismo segmento en la LAN.

En el switch, cualquier puerto puede pertenecer a una VLAN y los paquetes de unicast, broadcast y multicast que sean generados, serán enviados solo a las estaciones que pertenecen a esa VLAN. Para que la segmentación de los dominios de broadcast sea efectiva, cada VLAN debe pertenecer a una subred diferente. De esta forma se segmentan los dominios de broadcast por medio de las VLANs.

Por ejemplo, en la figura 1 se muestra un conjunto de hosts agrupados en 2 VLANs. Los hosts sólo pueden comunicarse con otros dispositivos que pertenezcan a su misma VLAN, es decir, los hosts de la VLAN de Contabilidad no pueden comunicarse con los de Marketing y viceversa.

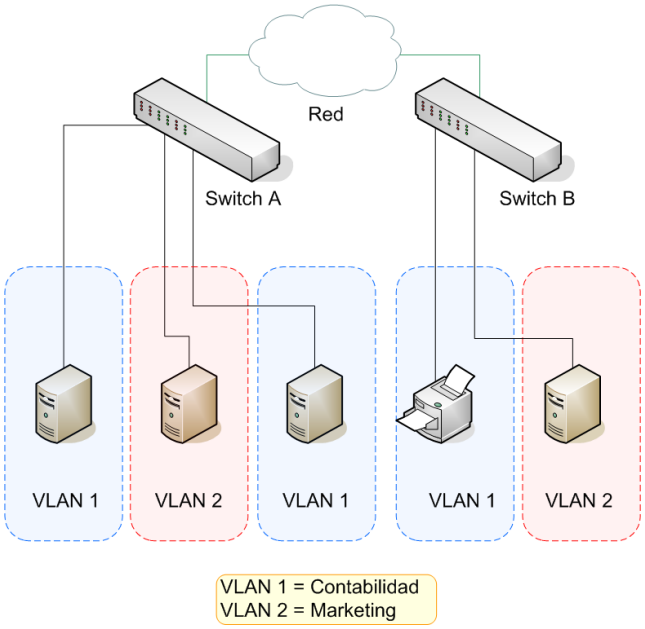


Figura 1. Red con hosts distribuidos en 2 VLANs

Generalmente, al utilizar la segmentación por VLAN se establece una relación de uno a uno entre la VLAN y la subred IP. A partir de la relación VLAN – subred, las VLANs ayudan a proveer servicios de segmentación, escalabilidad, seguridad y capacidades mejoradas de administración y control de tráfico dentro de la red.

Existen tres tipos de implementaciones de VLAN:

- Por direcciones MAC
- Basada en protocolos

- Basada en puertos

1.2. Tipos de VLAN

1.2.1. VLAN por Direcciones MAC

Actualmente, es muy rara la asignación de las VLANs por éste método, a pesar que es útil. Se asignan las direcciones MAC a las VLANs en el switch, y así, cuando el switch reciba una trama, busca en su tabla la dirección MAC y extrae la VLAN a la que pertenece.

Ventajas:

- ***Facilidad para el desplazamiento.*** Las estaciones pueden moverse a cualquier ubicación física perteneciendo siempre a la misma VLAN sin que se necesite ninguna reconfiguración del switch.

- ***Multiprotocolo.*** No presenta ningún problema de compatibilidad con los diversos protocolos y soporta incluso la utilización de protocolos dinámicos tipo DHCP.

Desventajas:

- ***Complejidad en la administración.*** Todos los hosts deben configurarse inicialmente en una VLAN. El administrador de la red introduce de forma manual, en la mayoría de los casos, todas las direcciones MAC de la red en algún tipo de base de datos. Cualquier cambio o el ingreso de un nuevo host, requiere modificar la base de datos. Todo esto puede complicarse extremadamente en redes con un gran número de usuarios o switches.

Existen soluciones alternativas para automatizar esta definición y normalmente se utiliza un servidor de configuración, de forma que las direcciones MAC se copian de las tablas de direcciones de los switches a la base de datos del servidor. La

asignación dinámica de las VLANs en base a la dirección MAC es posible, si bien su implementación puede ser muy compleja, es una excelente alternativa.

1.2.2. VLAN por Protocolo

Este método se configura igual que el método por direcciones MAC, excepto que se introducen en el switch las direcciones lógicas de los hosts. Su uso no es muy común, por el uso de servidores DHCP en las empresas, que asignan dinámicamente las direcciones IP a las computadoras.

La asignación a las VLANs se basa en información de protocolos de red (por ejemplo dirección IP o dirección IPX y tipo de encapsulamiento). La pertenencia a la VLAN, se basa en la utilización de filtros que se aplican a las tramas. Los filtros han de aplicarse por cada trama que entre por uno de los puertos del switch.

Ventajas:

- ***Segmentación por protocolo.*** Es el método apropiado solo en aquellas redes en las que el criterio de agrupación de usuarios esté basado en el protocolo de capa 3 (capa de red del modelo de referencia OSI), es decir, hay departamentos que trabajan en Token Ring, otros en Ethernet, etc y es mejor agruparlos por el protocolo de red que utilizan.

- ***Asignación dinámica.*** Tanto la definición de VLANs por dirección MAC como por protocolo de capa 3, ayudan a automatizar la configuración del puerto del switch en una VLAN determinada.

Desventajas:

- ***Problemas de rendimiento y control de broadcast.*** La utilización de VLANs de capa 3 requiere complejas búsquedas en tablas de pertenencia que afectan al rendimiento del switch. Los retardos de transmisión pueden aumentar entre un 50 % y un 80 % incrementando el nivel de latencia del dispositivo.

El problema de control de broadcast, surge con los dispositivos con múltiples protocolos o sistemas multistack (por ejemplo hosts con stacks TCP/IP, IPX y AppleTalk) que pertenecen a tantas VLANs como protocolos utilizan y por lo tanto recibirán todos los broadcast provenientes de las diversas VLANs en las que están incluidas.

- ***Equipo especializado.*** No todos los switches pueden trabajar en la capa 3, por lo que se deberá incurrir en gastos si no se poseen estos dispositivos. Además, los switches de capa 3 son más costosos que los switches tradicionales.

- ***No soporta protocolos de capa 2 ni protocolos dinámicos.*** El host necesita una dirección de capa 3 para que el switch lo asigne a una VLAN. Los hosts que utilicen protocolos que carecen de direccionamiento en capa 3, como NetBios y LAT, no podrán asignarse a una VLAN. Si existen protocolos dinámicos como DHCP y el host no tiene configurada su dirección IP ni puerta de enlace por defecto, el switch no podrá clasificar la estación dentro de una VLAN.

1.2.3. VLAN por Puerto

Es el método más común de configuración, en donde las VLANs son asignadas a puertos de forma individual, en grupos, en filas o a través de 2 o más switches. En comparación con los 2 métodos anteriores, es el más fácil de implementar y administrar.

Ventajas:

- ***Facilidad de movimientos y cambios.*** Un movimiento supone que la estación cambia de ubicación física pero sigue perteneciendo a la misma VLAN. Este cambio físico requiere de la reconfiguración del puerto al que se conecta el dispositivo, salvo si se utiliza la asignación dinámica de la VLAN. En un cambio de membresía a una nueva VLAN sin movimiento físico del dispositivo, el puerto del switch ha de configurarse como perteneciente a la

nueva VLAN. Puede ser que el dispositivo requiera una reconfiguración a nivel de direccionamiento (por ejemplo si se utiliza protocolo IP sin servidor DHCP). La reconfiguración del host no será necesaria si la subred (IP, IPX, etc.) a la que pertenece está totalmente contenida en la VLAN. Cualquier operación de añadir, mover o cambiar a un usuario se traduce normalmente en la reconfiguración de un puerto y algunas aplicaciones gráficas de gestión de VLANs automatizan completamente esta reasignación.

- ***Microsegmentación y contención del broadcast.*** Aunque los switches permiten dividir la red en pequeños segmentos, el tráfico broadcast sigue afectando al rendimiento de los dispositivos y se necesitan routers o VLANs para aislar los dominios de broadcast. La definición de VLANs por puerto implica que el tráfico de broadcast de una VLAN no afecta a los hosts en otras VLANs. El broadcast se contiene en la VLAN en que se origina.

- ***Multiprotocolo.*** La definición de VLANs por puerto es totalmente independiente del protocolo o protocolos utilizados por los hosts. No existen pues, limitaciones para protocolos de uso poco común como VINES, OSI, etc. o protocolos de configuración dinámica como DHCP.

Desventajas:

- ***Administración.*** Los movimientos y cambios implican normalmente una reasignación del puerto del switch a la VLAN a la que pertenece el host. Aunque las aplicaciones de gestión facilitan esta tarea, es recomendable combinar dichas aplicaciones con mecanismos de asignación dinámica de VLAN de forma que se asignan los puertos a la VLAN en función de la dirección MAC o de otros criterios como la dirección de nivel 3. Cisco ha desarrollado un método de asignación dinámica de red VLAN a puertos basándose en las direcciones MAC de las estaciones de red.

1.2.4. VLANs en Redes Inalámbricas

Es posible extender las VLANs a las redes inalámbricas por medio de un access point. Un access point es un receptor-transmisor de datos para redes inalámbricas, que utiliza ondas de radio para conectar una red cableada con dispositivos de red inalámbricos. Se puede relacionar con un hub que se comunica con dispositivos inalámbricos.

El access point segmenta la red inalámbrica relacionando a las VLANs con diferentes SSIDs y con llaves WEP. Un SSID es un código único que identifica una red inalámbrica, lo que permite a los dispositivos que tienen un mismo SSID, comunicarse entre ellos. Cada SSID se asocia solamente a una VLAN. El número máximo de SSIDs que se pueden configurar en un access point, indica la cantidad de VLANs que puede soportar. Por otro lado, las llaves WEP son utilizadas para cifrar la información que viaja entre dispositivos inalámbricos, y así, no sea posible que un intruso pueda comprender la información.
La figura muestra la diferencia entre la segmentación tradicional de una red física y la segmentación lógica de VLANs con dispositivos inalámbricos interconectados.

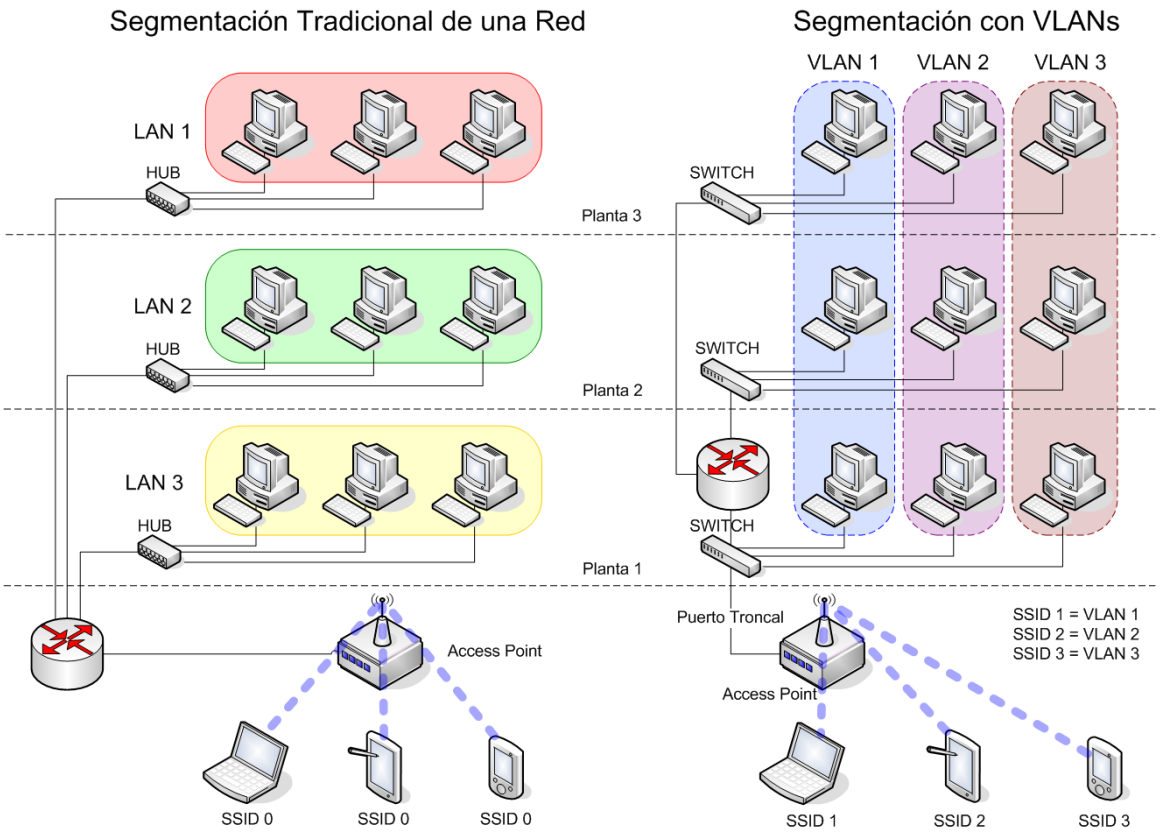


Figura 2. Comparación entre la segmentación tradicional de una red y una con VLANs.

1.2.4.1. Incorporando Dispositivos Inalámbricos a las VLANs

Los componentes básicos de una VLAN consisten en un access point y un cliente que utilice tecnología inalámbrica. El access point está físicamente conectado a través de un puerto troncal en un switch, donde las VLANs están configuradas.

En términos generales, la clave para que un access point pueda conectarse a una VLAN específica, es asociando un SSID al código de VLAN. Cuando esta conexión se ha realizado, los dispositivos de la red inalámbrica que tienen el mismo SSID, pueden acceder a otros dispositivos de la VLAN por medio del access point.

Es posible usar estas características de las VLANs, para organizar dispositivos inalámbricos con gran eficiencia y flexibilidad. Por ejemplo, un access point actualmente puede manejar los requerimientos específicos de múltiples usuarios,

teniendo una amplia variedad de accesos a la red y de permisos. Sin embargo, si no se contara con las VLANs, los access point agruparían a los dispositivos basados en el tipo de acceso y los permisos que les fueron asignados, como por ejemplo, filtros, políticas, listas de acceso, tablas de enrutamiento, etc.

Dos estrategias comunes para organizar VLANs inalámbricas son:

- *Segmentación por grupos de usuarios:* Es posible segmentar la red inalámbrica de la comunidad de usuarios y reforzar diferentes políticas de seguridad para cada grupo. Por ejemplo, se pueden crear tres VLANs cableadas y tres inalámbricas en un ambiente empresarial para empleados de tiempo completo o medio tiempo, y también proveer acceso a los invitados.
- *Segmentación por el tipo de dispositivo:* Se puede segmentar la red inalámbrica, para que permita diferentes dispositivos con distintas reglas de seguridad para ingresar a la red. Por ejemplo, algunos usuarios pueden tener dispositivos inalámbricos de mano (Pocket PC, Palms, laptops, etc) que soportan solamente WEP estáticos, y algunos otros usuarios pueden tener dispositivos más sofisticados que soportan WEP dinámicos. Es posible agrupar y aislar estos dispositivos en VLANs separadas.

1.2.4.2. Configurando VLANs en un Access Point

La configuración de un access point para que soporte VLANs, es un proceso de tres pasos:

1. Habilitar la VLAN en los puertos de radio y ethernet.
2. Asignando SSIDs a las VLANs.
3. Asignar las opciones de autenticación a los SSIDs.

Comenzando en modo privilegiado EXEC, siga los siguientes pasos para asignar un SSID a una VLAN y habilitar en el access point la VLAN en los puertos de radio y ethernet:

	Comandos	Propósito
Paso 1	**configure terminal**	Entra en modo de configuración global.
Paso 2	**interface dot11radio0**	Entra en modo de configuración de la interfaz para la interfaz del radio.
Paso 3	**ssid** *ssid-string*	Crea un SSID y entra en modo de configuración de SSID para el nuevo SSID. El SSID puede consistir de hasta 32 caracteres alfanuméricos. Los SSIDs son sensibles a mayúsculas y minúsculas. **Nota:** Se usa el comando **ssid** en las opciones de autenticación para configurar el tipo de autenticación para cada SSDI.
Paso 4	**vlan** *vlan-id*	(Opcional) Asigna el SSID a una VLAN en la red. Los dispositivos de los clientes que se asocian usando el SSID son agrupados en ésta VLAN. Ingrese el código de la VLAN a partir de 1 hasta 4095. Sólo se puede asignar una SSID a la VLAN.
Paso 5	**exit**	Regresa al modo de configuración de la interfaz para la interfaz de radio.
Paso 6	**interface dot11radio0.x**	Ingresa al modo de configuración de la interfaz para la subinterfaz de la VLAN de radio.
Paso 7	**encapsulation dot1q** *vlan-id* [**native**]	Habilita una VLAN en la interfaz de radio. (Opcional) Designa la VLAN como la VLAN de administración. En muchas redes, la VLAN de administración es la VLAN 1.
Paso 8	**exit**	Regresa al modo de configuración global.
Paso 9	**interface fastEthernet0.x**	Ingresa al modo de configuración de la interfaz para la subinterfaz de la VLAN ethernet.
Paso 10	**encapsulation dot1q** *vlan-id* [**native**]	Habilita una VLAN en la interfaz ethernet. (Opcional) Designa la VLAN como la VLAN de administración. En muchas redes, la VLAN de administración es la VLAN 1.
Paso 11	**end**	Regresa al modo privilegiado EXEC.
Paso 12	**copy running-config startup-config**	(Opcional) Guarda la configuración en el archivo de configuración.

Este ejemplo muestra como:

- Nombrar un SSID.
- Asignar el SSID a una VLAN.

- Habilitar la VLAN en los puertos de radio y ethernet como la VLAN administrativa.

```
ap1200# configure terminal
ap1200(config)# interface dot11radio0
ap1200(config-if)# ssid batman
ap1200(config-ssid)# vlan 1
ap1200(config-ssid)# exit
ap1200(config)# interface dot11radio0.1
ap1200(config-subif)# encapsulation dot1q 1 native
ap1200(config-subif)# exit
ap1200(config)# interface fastEthernet0.1
ap1200(config-subif)# encapsulation dot1q 1 native
ap1200(config-subif)# exit
ap1200(config)# end
```

1.3. Modos de Membresía de las VLAN por Puerto

Los modos de membresía de las VLANs por puerto, definen como los dispositivos de la red podrán acceder a las VLANs por los puertos de los switches. Como por ejemplo, se puede definir a cuantas VLANs se podrá tener acceso por determinado puerto del switch.

Los modos de membresías que se pueden configurar en los switches son:

- VLANs Estáticas
- VLANs Dinámicas
- Enlaces Troncales

Para configurar estos modos de membresía, es posible hacerlo a través de un software de configuración o a través del CLI de los switches.

1.3.1. VLANs Estáticas

En este modo de membresía, las VLANs se asignan directamente a los puertos de los switches por medio de un programa de administración de redes o por el CLI del switch. Cuando los puertos son configurados, mantienen la o las VLAN(s) hasta que el administrador del switch les asigne otra de forma manual. Por defecto, cuando a un puerto no se le ha configurado ninguna VLAN, pertenece a la VLAN 1, conocida inicialmente como la VLAN de administración.

Las VLANs estáticas cuya membresía se asignan estáticamente, trabajan bien cuando se cumple lo siguiente:

- Los movimientos de equipos son controlados y administrados.
- Existe un programa completo que administre las VLANs para configurar los puertos de los switches.
- No se asume que se requerirá gastos adicionales para el mantenimiento de las direcciones MAC de los dispositivos y de las tablas de filtrado.

En conclusión, las VLANs estáticas son adecuadas cuando la red no es muy grande y no hay mucho movimiento de hosts. Pero, podría llegar a ser muy complicado el mantenimiento para grandes redes que incluyen varios cientos o miles de hosts.

1.3.2. VLANs Dinámicas

Algunos switches poseen la propiedad de que a sus puertos se les puede asignar dinámicamente las VLANs. Esto es posible por medio de un Servidor de Administración de Políticas para VLANs (VMPS), el cual le envía al switch el nombre de la VLAN que debe asignarle al puerto que lo solicita. Además, para que el switch pueda trabajar de este modo, es necesario configurar sus puertos (o solamente algunos de éstos) como dinámicos y especificarle cual es la dirección del servidor VMPS (o servidores) al que debe consultar.

La comunicación entre el switch y el servidor VMPS se establece por medio de un protocolo llamado VQP (Protocolo de Consulta de VLANs). Por su parte, el VQP utiliza el protocolo UDP para trasportarse en la red, lo que lo hace rápido para llegar a su destino, sin embargo, éste no es confiable debido a que no tiene acuse de recibo por segmento.

Un puerto cambia de estado hacia activo cuando un dispositivo se conecta o enciende, pero no envía ningún tipo de tráfico desde la red al host, hasta que el servidor VMPS le asigne la VLAN. Si el enlace en el puerto dinámico se pierde, el puerto regresa a su estado natural de aislado y no pertenece a ninguna VLAN. Cuando la conexión entre el switch y el host se reestablece, el proceso de asignación de la VLAN al puerto se vuelve a llevar a cabo como si fuera por primera vez.

Existe un intervalo de reconfirmación de las VLANs asignadas. Este intervalo se configura en el switch (no todos poseen esta propiedad) y la función que desempeña es la de interrogar al VMPS cada cierto tiempo, para indagar si la VLAN que se le ha asignado a un puerto dinámico sigue siendo la misma. Si no lo es, el VMPS envía un mensaje con el nuevo nombre de la VLAN que debe asignarle al puerto o dependiendo del modo de seguridad del VMPS, desactivar el puerto o denegar el acceso al host.

Es de notar que cuando un puerto es configurado como dinámico, sólo puede pertenecer a una VLAN. Además, múltiples hosts pueden estar activos en un mismo puerto si todos ellos pertenecen a la misma VLAN. Sin embargo, el VMPS deshabilita un puerto dinámico si la cantidad de hosts permitidos es excedido. Por ejemplo, si hay más de 20 hosts activos en un puerto para un switch Catalyst 2950 o 3550, el VMPS deshabilitará el puerto. El total de hosts permitidos varía de plataforma en plataforma.

Existen algunas restricciones para que la asignación dinámica se lleve a cabo, entre ellas se mencionan las siguientes:

- El VMPS debe ser configurado antes de que los puertos se configuren como dinámicos.
- El dominio de administración VTP de los clientes del VMPS (switches) y del servidor VMPS debe ser el mismo.
- La VLAN de administración de los clientes del VMPS (switches) y del servidor VMPS debe ser la misma.
- Cuando un puerto es configurado como dinámico, la característica del spanning-tree Port Fast es automáticamente habilitada para ese puerto.
- Después de que un puerto estático es convertido a dinámico en la misma VLAN, el puerto se conecta inmediatamente a la VLAN hasta que el VMPS verifique la legalidad del host en el puerto.
- Los puertos estáticos que son troncales no pueden convertirse a dinámicos.
- Cuando un puerto estático posee una MAC asociada, el dispositivo de esa MAC no podrá ingresar en un puerto configurado como dinámico.
- El switch deshabilita un puerto cuando existen demasiados hosts activos en ese puerto (el número de hosts permitidos depende del modelo del switch).

1.3.3. Enlaces Troncales

En este modo, los puertos del switch pueden configurarse para funcionar de dos maneras. La primera es el *modo de acceso*, en donde un puerto pertenece a una sola VLAN. La segunda es cuando está configurado como *enlace troncal*, este puede soportar el tráfico de múltiples VLANs, ya que el puerto troncal no pertenece a ninguna VLAN en específico.

Por norma se seleccionan para la función de los enlaces troncales, los puertos con mayor capacidad de ancho de banda disponible. Por ejemplo, los puertos que permiten ser configurados como troncales en los switches Catalyst son los Fast Ethernet, Gigabit Ethernet y los 10 Gigabit Ethernet.

Un enlace troncal es un enlace punto a punto que puede portar múltiples VLANs. Esto permite que sea posible extenderlas hacia toda la red. De no existir enlaces

troncales, se debe utilizar un enlace físico por cada VLAN entre los dispositivos que transporten el tráfico. Por lo tanto, un enlace troncal ahorra puertos al momento de enlazar dispositivos que implementan VLANs.

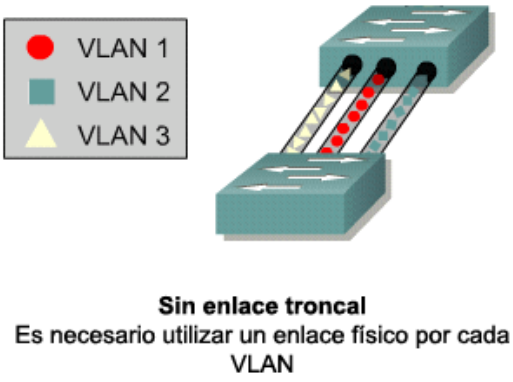


Figura 3.1 Interconexión de Switches sin troncales

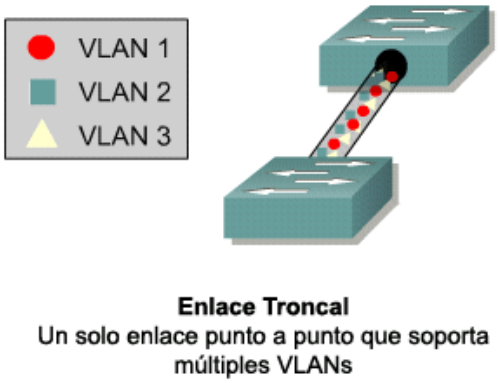


Figura 3.2 Interconexión de Switches utilizando troncales

Existen diferentes mecanismos para que múltiples VLAN puedan ser transportadas en un solo enlace. Uno de estos mecanismos es el de filtrado de tramas, que funciona por medio de una tabla de filtrado desarrollada para cada switch. Los switches intercambian las entradas de la tabla de filtrado, las cuales contienen la relación entre los dispositivos y las VLANs. Luego, las tramas entrantes son comparadas con las direcciones de la tabla para ser filtradas. El segundo mecanismo, es el de identificación de tramas, el cuál provee una solución escalable para la implementación de las VLAN. En la identificación de tramas existen dos formas comúnmente utilizadas en los segmentos Ethernet: el protocolo propietario Inter-Switch Link (ISL) y el estándar IEEE 802.1Q.

El protocolo ISL encapsula las tramas al momento que viajan en los enlaces troncales. Se realiza el encapsulamiento, anteponiendo un encabezado de 26 bytes a la trama y al final de esta se agrega un campo CRC de 4 bytes como verificación de redundancia cíclica. El encabezado ISL contiene la identificación de la VLAN y se agrega únicamente cuando la trama se transmite a través de un puerto configurado como enlace troncal. El encabezado ISL es removido cuando la trama se envía por un puerto de acceso.

El protocolo IEEE 802.1Q funciona insertando un campo identificador en el encabezado existente de la trama, este proceso se llama identificación interna (internal tagging).

“Los objetivos de la identificación de la trama según el estándar IEEE 802.3 son los siguientes:

- Permitir la adición de información de prioridad de usuario en una trama IEEE 802 LAN que carecen de la capacidad de señalar prioridad a nivel MAC
- Permitir a las tramas contener un Identificador de VLAN (VID)”[1]

Durante el proceso de identificación se inserta la marca (tag) después de las direcciones MAC destino y origen de una trama ethernet. Finalmente, se recalcula la secuencia de verificación de la trama (FCS).

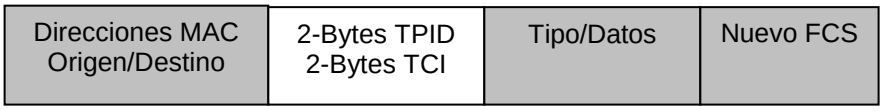


Figura 3. Formato de Trama IEEE 802.3 (ethernet) marcado con IEEE 802.1Q

El encabezado IEEE 802.1Q contiene 4 Bytes divididos entre dos campos, los cuales representan lo siguiente:

1. Identificador de marca - TPID (2 Bytes)	Contiene un valor fijo de “0x8100“ que indica que la trama transporta información del protocolo 802.1Q
2. Información de control de marca - TCI (2 Bytes)	Contiene: indicador de prioridad de usuario (3bits), indicador de formato canónico de (1bit), identificador de VLAN (12bits).

(IEEE Standards, IEEE Std 802.1Q, 2003)

1.3.3.1. Introducción al VTP

El Protocolo Troncal de VLAN (VTP) ha sido diseñado con el fin de reducir la carga administrativa en las redes conmutadas que implementan VLANs. Su función es la de mantener la configuración de las VLANs al brindar una forma de administrar la adición, eliminación y renombramiento de estas en el ámbito de toda la red. Con el VTP se minimizan los problemas generados al configurar los switches de forma manual. Uno de estos problemas es la interconexión de VLANs causado por inconsistencias de configuración como utilizar nombres duplicados para identificar a diferentes VLANs. También pueden suceder problemas como la desconexión interna de la VLAN al intercambiarse el tipo de LAN a otro por ejemplo de Ethernet hacia FDDI.

Los beneficios que se obtienen con el uso del VTP son los siguientes:

- Consistencia en la configuración de VLAN a través de la red.
- Esquema de mapeo que permite a las VLANs ser transportadas sobre una mezcla de medios.
- Monitoreo y control de VLANs.
- Reporte dinámico de las VLANs agregadas a lo largo de la red.
- Configuración automática de los dispositivos al agregar una nueva VLAN.

El VTP es un protocolo de mensajería que trabaja en la capa de enlace de datos del modelo OSI. Cuando se transmiten mensajes VTP hacia otros switches de la red, el VTP puede ser encapsulado en una trama de protocolo de troncal, como ISL o IEEE 802.1Q. Comúnmente, se pueden encontrar cuatro campos similares en los mensajes VTP:

Versión de Protocolo VTP	Versión 1 ó 2
Tipo de Mensaje VTP	Indica 1 de 4 tipos diferentes
Longitud del nombre de dominio administrativo	Indica el tamaño del nombre a continuación

Nombre del dominio administrativo VTP	El nombre configurado como dominio administrativo

1.3.3.2. Modos de Operación del Switch

Los switches VTP pueden funcionar en cualquiera de tres modos: servidor, cliente o transparente.

Servidor	Puede crear, modificar y eliminar VLANs, además de parámetros de configuración de VLANs para todo el dominio VTP. Los mensajes VTP son enviados a través de todos los puertos troncales. Los servidores VTP almacenan la información en la memoria no volátil del switch.
Cliente	Estos no pueden crear, modificar o eliminar información de VLANs. El único rol de los clientes VTP es de procesar todos los cambios de VLAN y enviar mensajes VTP a través de todos los puertos configurados como troncales.
Transparente	Los switches configurados en modo transparente solamente envían los anuncios VTP pero ignoran la información contenida en el mensaje. Un switch transparente no modifica su base de datos cuando recibe una actualización de VLAN.

1.4. Beneficios que brinda la implementación de las VLAN

La reducción en los costos de administración es un punto crucial para toda empresa, y es observable en el tiempo que los administradores de red consumen en las modificaciones que estas sufren. Con la necesidad de añadir, mover o retirar dispositivos dentro de un edificio o campus, es necesario mantener cierta cantidad de personal disponible para atenderlos, pero con el uso de las VLANs, no siempre será necesario hacer alguna modificación en la configuración de los equipos, y la cantidad de personal podría disminuir. Además, concentrará a los administradores de redes,

en tareas más vitales tales como lo son el análisis, mejoramiento y el monitoreo del desempeño de la red.

En lo que a seguridad respecta, el establecimiento de grupos de usuarios, evita que individuos ajenos a los grupos, puedan tener acceso a información vital de servidores u otros dispositivos en la red. Por lo que si los usuarios pertenecen a VLANs, sólo tendrán acceso a los dispositivos que pertenezcan a esa VLAN.

A menudo, muchos usuarios que tienen acceso al Internet o reciben correos electrónicos infectados con virus generan un mayor tráfico en la red, porque existe una gran cantidad de virus en donde su intención primordial es el envío información de la computadora en donde está instalado al Internet o el de tratar de propagarse en la red, buscando en todas las máquinas posibles algún tipo de “agujero” para instalarse y comenzar a enviar tráfico. Así, este tipo de virus solamente podrán afectar el desempeño de la VLAN y no de la red en general, lo que será más sencillo de solventar.

Otro de los beneficios que se obtienen con el uso de las VLANs es que hacen de contención de los dominios de broadcasts, lo que mejora el desempeño de toda la red, pues los paquetes broadcast solo son recibidos por los dispositivos que pertenecen a la VLAN y se logra que los dispositivos obtengan un mayor ancho de banda para transmitir la información.

Como es normal en todas las redes, el crecimiento puede perjudicar en gran medida su desempeño, dejándola sin el ancho de banda requerido para trabajar normalmente, lo que llevaría a hacer inversiones costosas. Pero el uso de las VLANs, ayuda a que ese crecimiento se haga de una manera controlada, en donde el ingreso de nuevos dispositivos puede hacerse dentro de las VLANs existentes o si es necesario, se pueden crear otras si están muy saturadas.

1.5. Recomendaciones en el diseño de redes con VLANs

Una VLAN se describe como un grupo de dispositivos con un conjunto común de requerimientos, estos dispositivos se comunican entre sí como si estuviesen conectados al mismo medio, sin importar su ubicación física. Con el fin de incrementar el desempeño de la red, la agrupación de los dispositivos debe de estar definida en base a parámetros como funciones organizacionales, grupos de proyectos, o requerimientos de aplicaciones en lugar de estar basados en cercanía física o agrupación geográfica. Las VLANs brindan la oportunidad de que grupos geográficamente dispersos estén interconectados sin importar sus conexiones físicas a la red, la reconfiguración se hace con herramientas de software y no con el movimiento físico de los equipos.

Uno de los objetivos para la implementación de las VLANs es el de brindar los servicios de segmentación que normalmente ofrecen los enrutadores, por lo que a cada VLAN se le debe asignar una dirección de subred única en la red. Al igual que con los segmentos de red LAN que son interconectados por los enrutadores, los mismos enrutadores son los encargados de brindar la conectividad entre los segmentos de las VLANs. De no ser así, se violaría la integridad del dominio de broadcast de VLAN.

1.5.1. Diseño de Redes de Campus

El término redes de campus fue utilizado inicialmente para describir a las redes que se desarrollaban en los campus universitarios. El campus es un conjunto de terrenos y edificios pertenecientes a una universidad o empresa. Actualmente, el término red de campus ha evolucionado para describir campus corporativos. Se utiliza para nombrar una red que se extiende entre distintos edificios de empresas, universidades o dentro de un área industrial y puede consistir de varias LANs. En la topología de las redes de campus, generalmente se utilizan tecnologías LAN tales como Ethernet / Fast Ethernet / Gigabit Ethernet, Token Ring, FDDI y ATM. Una red grande con grupos de edificios puede también utilizar tecnologías WAN para la interconexión de

los edificios. El tamaño de la red de campus, los requerimientos en disponibilidad y desempeño de la red, son algunos de los factores importantes que influyen en el diseño.

1.5.1.1. Principios Generales de Diseño de Redes

El diseño de las redes se debe enfocar a cumplir los siguientes requisitos:

Escalabilidad	Prever el crecimiento en el número de usuarios y en la cantidad de datos a transportar. La red debe de tener la capacidad de ser actualizada sin tener que cambiar completamente a los dispositivos que la conforman.
Funcionalidad	Debe de soportar las aplicaciones y el flujo de datos requerido.
Desempeño	Incluye tres métricas importantes: tiempo de respuesta, volumen y utilización.
Disponibilidad	Se requiere que la disponibilidad sea cercana al 100%.
Administrabilidad	La red debe de permitir monitoreo y ser administrable.
Control de Costos	El diseñador debe de obtener el máximo nivel de efectividad con las limitaciones de presupuesto existentes, debe de existir un balance entre costo y efectividad.

Tabla 1. Fuente: CCDP Student Guide

1.5.2. Diseño Jerárquico por Capas

Los modelos jerárquicos permiten dividir la complejidad del diseño de redes en diferentes capas. Cada una de estas capas brinda funciones diferentes, permitiendo así, que el diseñador pueda seleccionar los dispositivos y sus características para cada capa. El uso de diferentes capas también facilita realizar cambios en la red al

brindar niveles de aislamiento entre las capas. Finalmente, el uso de capas en el diseño brinda a los administradores de red, una forma de comprender fácilmente los puntos de transición en la red lo que también ayuda a identificar puntos donde ocurran fallas.

El diseño jerárquico de redes presenta tres capas: núcleo, distribución y la capa de acceso. Cada una de estas capas brinda una función específica en la red de campus.

- El núcleo es la capa que provee de un transporte óptimo entre los sitios.
- La capa de distribución brinda conectividad basada en políticas.
- La capa de acceso se encarga de dar acceso a los grupos de trabajo o a los usuarios.

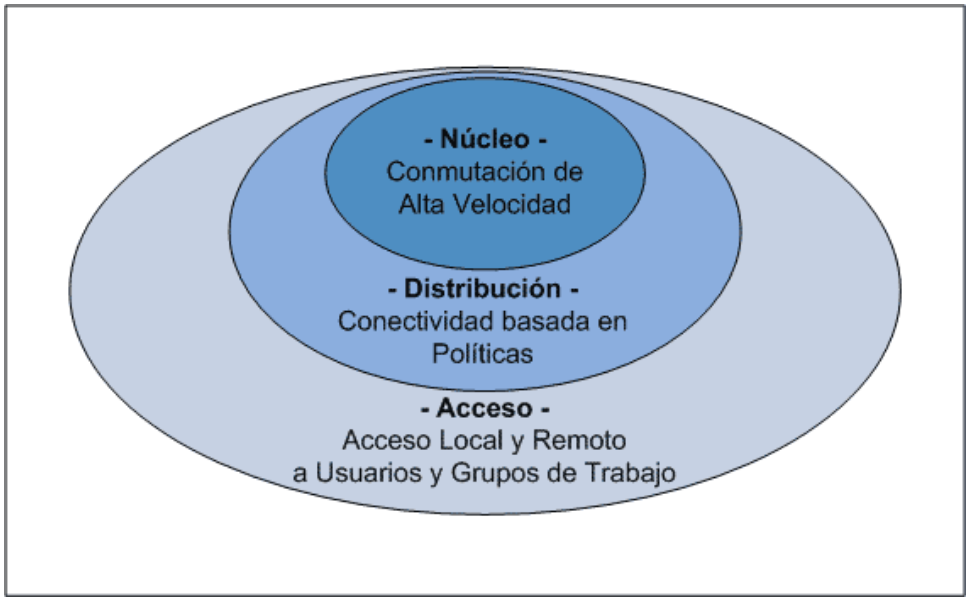


Figura 4. Capas del diseño jerárquico.

1.5.2.1. Capa de Núcleo

La capa de núcleo es un backbone de conmutación de alta velocidad y debe de ser diseñada para conmutar paquetes lo más rápido posible entre todos los dispositivos de la capa de distribución. El núcleo no debe de manipular paquetes, como filtrar por medio de listas de acceso, ya que disminuiría la velocidad del proceso de conmutación. Es normal que los núcleos sean conformados por equipos de

conmutación de capa de red. Las VLANs y los troncales de VLANs no están presentes en el núcleo.

1.5.2.2. Capa de Distribución

La capa de distribución se encuentra entre el núcleo y la capa de acceso. Esta es la encargada de manipular los paquetes y definir una frontera hacia el núcleo. La capa de distribución es la encargada además de otras funciones como:

- Adición de áreas o direcciones
- Conectividad de los departamentos o grupos de trabajo al backbone
- Enrutamiento entre VLANs
- Cualquier tipo de transiciones de medios
- Seguridad

La capa de distribución también puede ser el punto en que sitios remotos accedan a la red corporativa. Finalmente, en esta capa se realizan manipulación de paquetes, además brinda conectividad en base a políticas.

1.5.2.3. Capa de Acceso

En la capa de acceso es donde los usuarios finales son autorizados en la red. Aquí, es donde aparecen las listas de acceso para optimizar los requerimientos de grupos específicos de usuarios. A continuación se presentan las funciones de la capa de acceso:

- Ancho de banda compartido
- Ancho de banda conmutado
- Filtrado por direcciones MAC
- Microsegmentación

En otros ambientes la capa de acceso puede brindar acceso desde sitios remotos a la red corporativa por medio de tecnologías de área amplia tales como la red pública telefónica (PSTN), Frame Relay, ISDN, DSL o por medio de enlaces dedicados.
La concepción o pensamiento que estas tres capas deben de existir en claras y distintas entidades es errónea. El modelo jerárquico ha sido concebido con el fin de ayudar al diseño de red y de representar las funciones que deben de existir en la red. La forma en que se implemente el diseño jerárquico depende de las necesidades de la red que se este diseñando.

1.5.3. La regla tradicional 80/20 para el tráfico de red

Idealmente los usuarios con intereses en común o patrones de trabajo relacionados se agrupan y se ubican en el mismo segmento de red. A este segmento lógico se agregan los servidores que sean indispensables para el grupo. De esta forma, se pretende minimizar en lo posible la carga en el backbone de la red.

En el esquema 80/20 se pretende por medio de la agrupación de usuarios y la ubicación de servidores en el mismo segmento lógico, se mantenga el mayor porcentaje posible de tráfico local dentro del mismo segmento. La regla 80/20 establece que en una red bien diseñada el 80% del tráfico sea local y no más del 20% de tráfico fluya hacia el backbone. La congestión del backbone es un indicador que los patrones de tráfico en la red no cumplen con la regla 80/20.

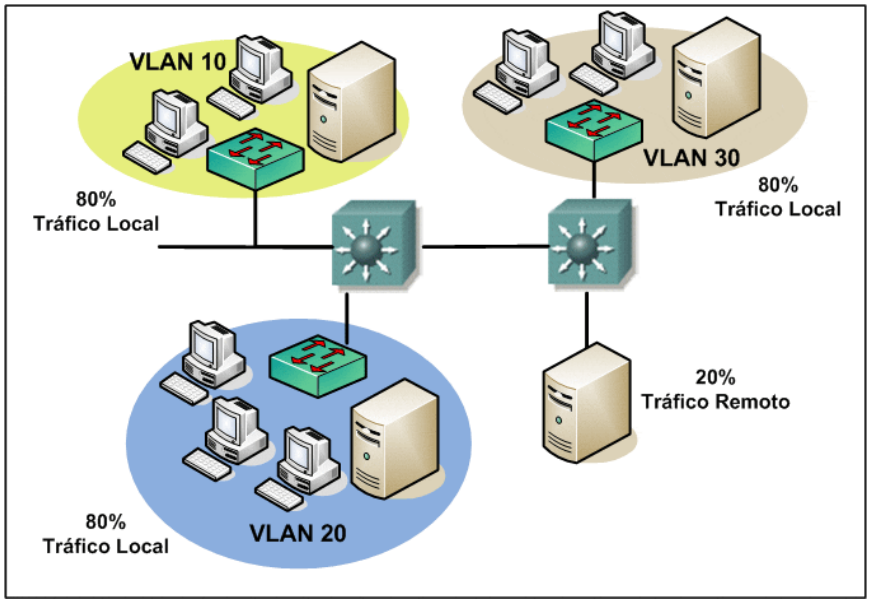


Figura 5. Esquema 80/20

1.5.3.1. VLAN de Extremo a Extremo

En el diseño de redes, las VLANs de extremo a extremo o VLANs de campus, están relacionadas con la regla 80/20. Se pretende que con el diseño de VLAN de extremo a extremo el tráfico en la red debe de permanecer en un 80% dentro de la VLAN y salir de ella a lo sumo un 20%. Las redes VLAN de extremo a extremo permiten que los dispositivos estén agrupados en base a la utilización de servidores, grupos de proyectos y departamentos.

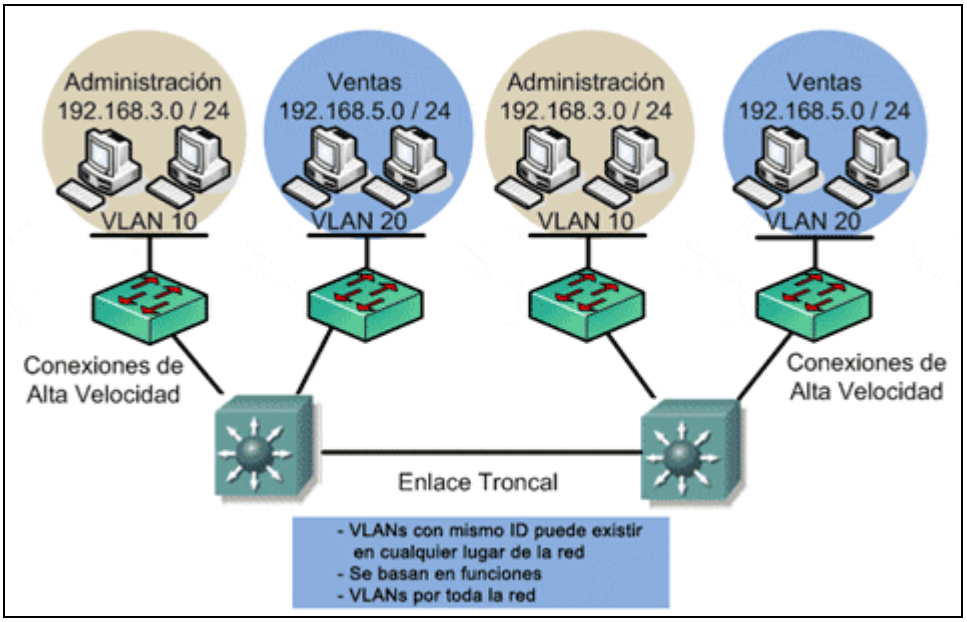


Figura 6. Diseño VLANs de Extremo a Extremo - 80/20

1.5.4. La regla 20/80

La migración hacia sistemas centralizados en Intranets Corporativas, servicios basados en Internet disponibles a toda la red empresarial y cambios en los esquemas organizacionales son algunas de las tendencias que transforman los patrones de tráfico en las redes actuales. Un modelo que ilustra estos cambios es el llamado 20/80 en el que un 20% del tráfico se mantiene local dentro del grupo de trabajo y el 80% sale de la red local hacia el núcleo del backbone o hacia fuera de la red.

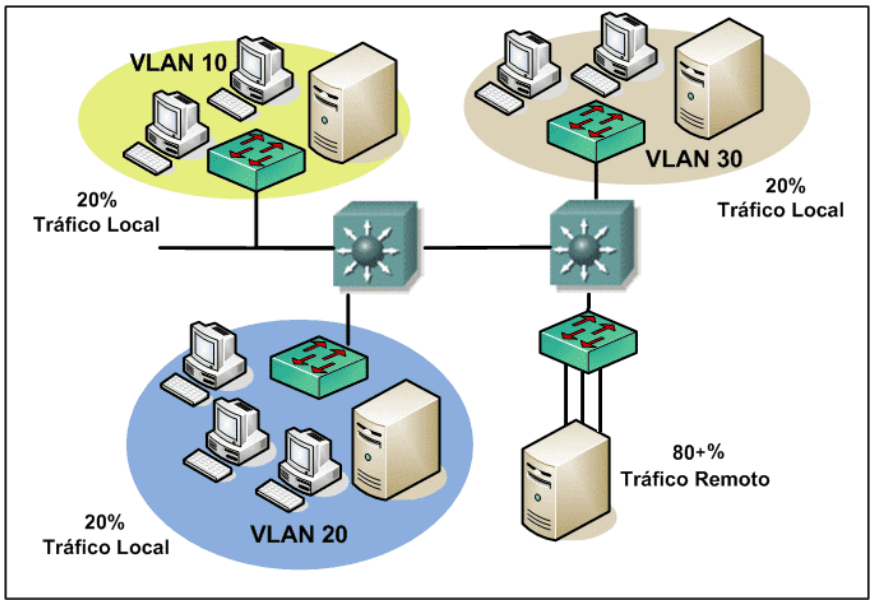


Figura 7. Esquema 20/80

Los factores que contribuyen al cambio en el flujo de tráfico de las redes corporativas son enumerados a continuación:

1. Influencia de las tecnologías de Internet y computación basada en la Web.
    - Existen fuentes de información diversas y están distribuidas, en lo que conocemos como los documentos de hipertexto.
    - La información está en constante desarrollo, evolución y fluye en distintos caminos.

2. Influencias provenientes de nuevos esquemas de organización en las empresas
    - Cambios de las estructuras organizacionales verticales con esquemas funcionales o lineales hacia la organización horizontal o plana en la que se trabaja en grupos y se disminuye la supervisión administrativa.
    - La existencia en la organización de grupos con funciones cruzadas o con esquemas de organización matricial las cuales están caracterizadas por la cooperación entre departamentos en proyectos específicos.
    - La cantidad de tráfico que viaja por el backbone se incrementa gracias a recursos compartidos a nivel corporativo, también por el flujo de información que se transmite entre los distintos grupos de trabajo.
3. El surgimiento de estructuras consolidadas de servidores y servicios llamadas granjas de servidores
    - El camino hacia la centralización de recursos informáticos declina el tráfico a nivel local de grupos de trabajo y lo traslada al núcleo de la red.
    - Las empresas buscan la implementación de las granjas de servidores por la seguridad, facilidad de administración y la disminución del costo de propiedad.
    - Todo el tráfico que va desde las subredes hacia las granjas de servidores atraviesa el backbone.

Para dar solución a las necesidades que provienen de los cambios en los patrones actuales de tráfico y las tendencias de integración en las organizaciones actuales, se requiere de una mayor eficiencia en los dispositivos de capa de red. Ya que estos dispositivos son los encargados de unir a los grupos de trabajo, distribuir y enrutar el tráfico desde las distintas subredes que forman la red corporativa. Existen equipos de red llamados switches multicapa que mejoran el desempeño de la conmutación a nivel de capa 3 igualándolo al de la capa 2 que normalmente se implementa a nivel de hardware por medio de circuitos electrónicos especializados llamados Circuitos Integrados de Aplicación Específica (ASIC). Con el desempeño mejorado de los procesos de conmutación en la capa 3, se disminuye el nivel de latencia entre las

subredes y se vuelve más práctico involucrar routers para la segmentación y conmutación de alta velocidad en las redes empresariales.

1.5.4.1. VLAN Local

Las VLANs locales se implementan en los bloques de switches de la capa de acceso y se basan en la ubicación física de los usuarios. Los usuarios miembros de un grupo de trabajo o de un departamento están en la misma VLAN y son miembros de la misma subred si los switches que les dan acceso a la red, están conectados al mismo switch de capa de distribución. En el caso que los usuarios del mismo departamento no estén conectados al mismo switch de distribución entonces son asignados un VLANID diferente y otra dirección de subred sin importar a que departamento pertenecen a nivel corporativo.

El modelo de VLAN local es más fácil de manejar y conceptualizar que el de las VLANs de extremo a extremo, que cubren diversas áreas geográficas. Las VLANs de extremo a extremo crean problemas con el protocolo spanning-tree, ya que extienden los dominios y muchas veces generan bucles, esto puede disminuir el tiempo de convergencia del protocolo y afectar la red en futuras ocasiones de fallas. Se recomienda evitar en lo posible los bucles o lazos restringiendo las VLANs localmente a un switch para minimizar la complejidad del diseño, incrementando de esta forma la facilidad para administrar la red. Con la disminución del área de aplicación de las VLANs mediante la adición de routers para manipulación de tráfico en capa 3, se obtienen dominios de spanning-tree más pequeños que convergen rápidamente en el caso de alguna falla. Debe de existir un balance en el diseño de redes de campus con referencia a la organización lógica, ad de la red y con los dispositivos físicos y la ubicación geográfica de los mismos.

1.6. Puntos principales y comentarios

En este capítulo se habló acerca de las VLANs, los tipos que existen y acerca del diseño de éstas. De modo que, a continuación se destacan los puntos más importantes:

- Las VLANs son agrupaciones lógicas de los dispositivos de una red, que definen los dispositivos que podrán comunicarse, sin importar el lugar geográfico en que se encuentren.

- Las VLANs ayudan a proveer servicios de segmentación, escalabilidad, seguridad y capacidades mejoradas de administración y control de tráfico dentro de la red.

- Existen tres tipos de implementaciones de VLAN, las cuales son: por direcciones MAC, basada en protocolos y basada en puertos.

- Las VLANs también se pueden extender a dispositivos inalámbricos por medio de los access point, como por ejemplo: laptops con tarjetas inalámbricas, Palms, Tablet PC's, lectores de códigos de barra, etc. Un access point es un receptor-transmisor de datos para redes inalámbricas, que utiliza ondas de radio para conectar una red cableada con dispositivos de red inalámbricos.

- En una red inalámbrica, un SSID es un código único que identifica una red inalámbrica, lo que permite a los dispositivos que tienen un mismo SSID, comunicarse entre ellos. Cada SSID se asocia solamente a una VLAN.

- Los puertos de los switches pueden ser configurados como estáticos, dinámicos o troncales, para que los hosts puedan ingresar a las VLANs. En los estáticos, el administrador de la red le asigna la VLAN manualmente. En los dinámicos, un servidor VMPS asigna el nombre de la VLAN a la que debe pertenecer el puerto. Por último, los puertos troncales pueden pertenecer a más de una VLAN y así poder extenderlas hacia toda la red.

- El diseño de las redes se debe enfocar a cumplir los siguientes requisitos: escalabilidad, funcionalidad, desempeño, disponibilidad, administrabilidad y control de costos.

CAPITULO II

2. SERVIDORES DE ADMINISTRACIÓN DE POLÍTICAS PARA VLANS

2.1. Introducción

En éste capítulo se describen los Servidores de Administración de Políticas para VLANs (VMPS); sus componentes y funcionamiento. Además, se explica la manera en que los servidores VMPS intercambian mensajes con los switches, por medio del protocolo VQP. Los componentes del VMPS que se explican son el archivo de configuración y el protocolo VQP. Asimismo, se detallarán los efectos en las tomas de decisiones del VMPS, por los cambios realizados en su configuración.

2.2. Que son los servidores VMPS

Los Servidores de Administración de Políticas para VLANs (VMPS) se encargan de asignar dinámicamente los puertos de switches a VLANs, basados en la información ingresada en su base de datos. Esto es posible solamente en aquellos switches en que sus puertos estén configurados como dinámicos.

Normalmente, al iniciar el VMPS comienza a bajar la base de datos con las relaciones de las direcciones MAC-a-VLANs desde un TFTP. La base de datos es un archivo de texto en formato ASCII, en donde se encuentran las políticas de permisos de los hosts a las VLANS y sus parámetros de operación. Una vez descargada, el VMPS lo interpreta línea por línea cargándola en memoria. En caso de ser necesario de agregar nuevas políticas en el archivo, el VMPS deberá cargar nuevamente toda la base de datos a fin de actualizar el cambio. Una vez hecho esto, el VMPS puede comenzar a procesar las peticiones de los clientes.

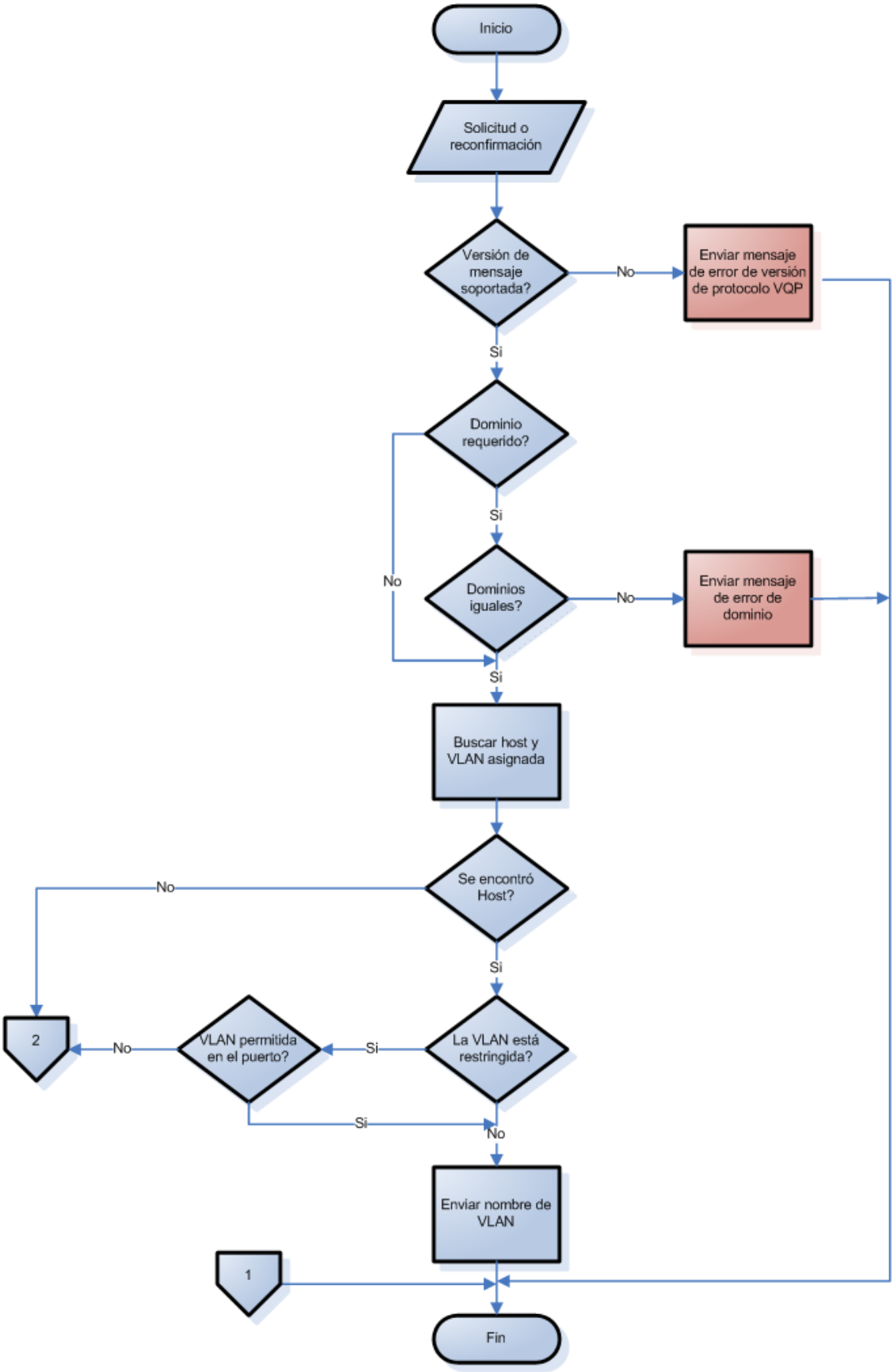
```
!vmps domain <domain-name>
! The VMPS domain must be defined.
!vmps mode { open | secure }
! The default mode is open.
!vmps fallback <vlan-name>
!vmps no-domain-req { allow | deny }
!
! The default value is allow.

vmps domain KRYPTOS
vmps mode open
vmps fallback --NONE--
vmps no-domain-req deny

!
!MAC Addresses
!
vmps-mac-addrs
!
! address <addr> vlan-name <vlan_name>
```

Figura 8. Ejemplo del archivo de políticas de permisos del VMPS.

Cuando un host se conecta al puerto de un switch que trabaja en modo dinámico, el switch envía una consulta al VMPS para obtener la VLAN a la que debe darle acceso. Si la petición es válida, el VMPS busca en su base de datos la dirección MAC del host y extrae la VLAN asignada. Si la VLAN está restringida a un grupo de puertos, entonces compara el puerto en el que está conectado el host contra el grupo de puertos. Si la VLAN está permitida para ese puerto, el VMPS la envía al cliente, de lo contrario el VMPS le envía un mensaje de acceso denegado o de deshabilitar el puerto, dependiendo del modo de seguridad en el que éste se encuentre trabajando (no seguro o seguro).

Un administrador de red también puede negar el acceso a una dirección MAC, por razones de seguridad, asignándole --NONE-- como nombre de VLAN.

En la siguiente página, se muestra el diagrama de flujo que sigue el VMPS para responder a las solicitudes y reconfirmaciones de los switches.


Inicio
Solicitud o reconfirmación
Versión de mensaje soportada?
No
Enviar mensaje de error de versión de protocolo VQP
Si
Dominio requerido?
Si
No
Dominios iguales?
No
Enviar mensaje de error de dominio
Si
Buscar host y VLAN asignada
Se encontró Host?
No
Si
2
No
VLAN permitida en el puerto?
Si
La VLAN está restringida?
Si
No
Enviar nombre de VLAN
1
Fin

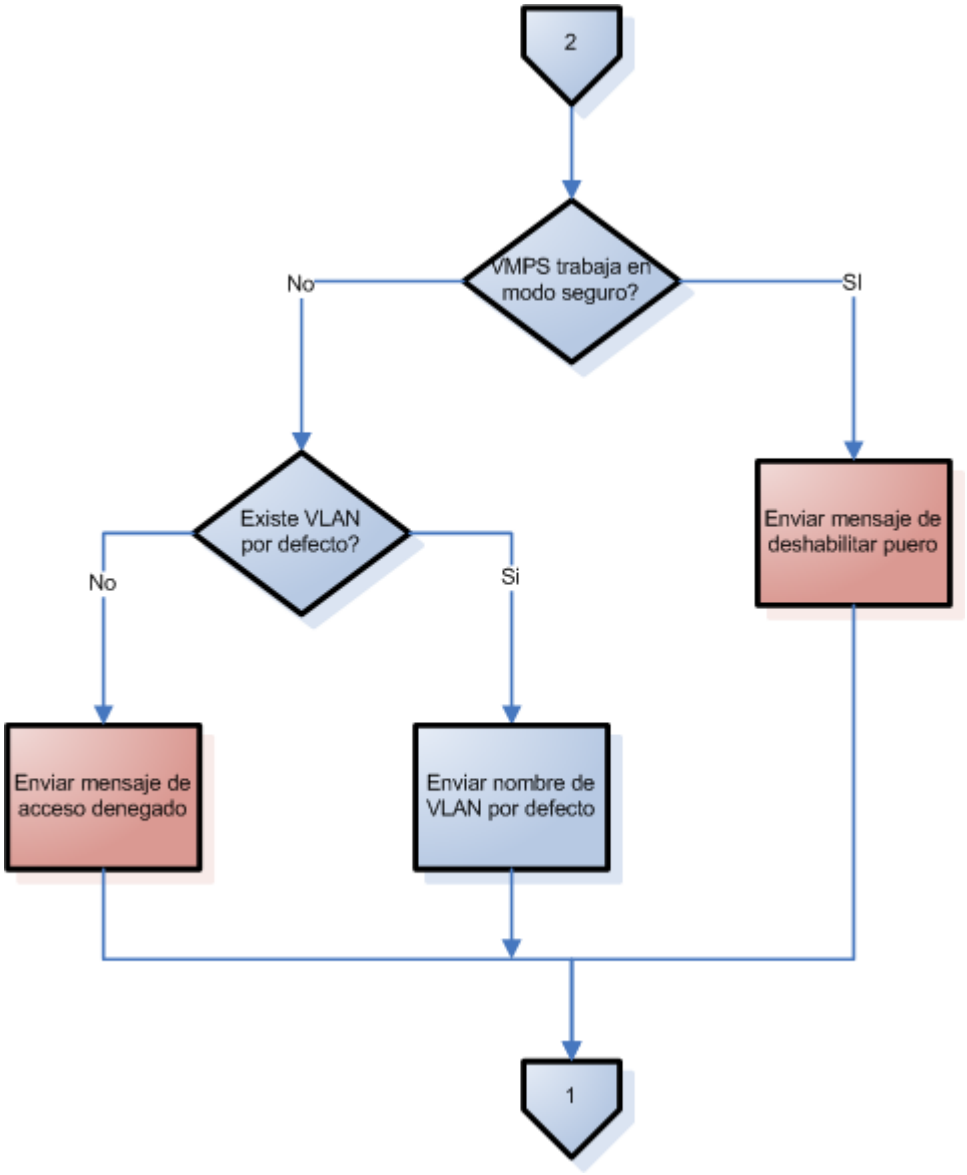


Figura 9. Diagrama de flujo que sigue el VMPS para responder solicitudes y reconfirmaciones de los switches.

El VMPS abre un puerto (socket) UDP para recibir las peticiones de los switches. El número de puerto destinado para este propósito es el 1589. Por dicho puerto, el VMPS escucha las peticiones de los clientes y les envía los mensajes de respuesta. La mensajería se lleva a cabo por un protocolo llamado VQP (Protocolo de Consulta de VLANs), que utiliza al protocolo UDP para transportase por la red.

Para que los switches en una red puedan comunicarse con un servidor VMPS, es necesario que se cumpla lo siguiente:

- Si se especifica en el archivo de configuración, el dominio de administración VTP de los clientes del VMPS (switches) y del servidor VMPS debe ser el mismo. Esto es útil cuando se tiene más de un VMPS en la red.
- La VLAN de administración de los clientes del VMPS (switches) y del servidor VMPS debe ser la misma.

2.3. Modo de seguridad del VMPS

El modo de seguridad determina que acción debe tomar el VMPS cuando un host no tiene acceso a una VLAN en un puerto del switch. Si el VMPS trabaja en modo seguro, le envía un mensaje al switch para deshabilitar el puerto. Si el VMPS trabaja en modo no seguro, le envía un mensaje al switch de acceso denegado al puerto, manteniendo el puerto aún activo.

2.3.1. Modo Seguro

Cuando el VMPS se encuentra trabajando en modo seguro, para todas las peticiones que reciba en las cuales los hosts no tengan permiso de ingresar a las VLANs, enviará mensajes a los switches clientes para deshabilitar el puerto. Esto implica, que el switch ya no escuchará o monitoreará ningún tipo de tráfico en dicho puerto, por lo que impide que el host ingrese a la red. Pero a su vez, evita que usuarios mal intencionados puedan ingresar a la red utilizando algún software para acceder ilegalmente o que puedan mantener ocupado al switch, evitando así problemas de desempeño por parte de éste. Cuando otro host requiera ingresar en el puerto deshabilitado, es necesario que el puerto sea manualmente rehabilitado[1] usando el CLI, aplicaciones de administración del switch o por medio de SNMP.

[1] *Esto es según la documentación de Cisco (Software Configuration Guide-Release 5.2 y Curriculum CCNP), sin embargo, en pruebas realizadas con un switch Catalyst 1900, se descubrió que al desconectar y conectar otra computadora, el switch vuelve a habilitar el puerto en vez de dejarlo apagado. Al parecer el modo seguro trabaja de diferente forma según la versión del switch e IOS.*

2.3.2. Modo No Seguro

Si el VMPS opera en modo no seguro, enviará un mensaje de acceso denegado al switch cliente cuando un host no tenga permiso de ingresar a la VLAN. Sin embargo, el switch continuará monitoreando el tráfico que vaya hacia el puerto y cuando este detecte una nueva dirección MAC en el puerto, volverá a hacer una nueva petición al VMPS.

2.4. Descripción del Archivo de Políticas a las VLANs

Este archivo es el que actualmente utiliza el VMPS como base de datos para guardar las políticas de los hosts a las VLANs. Como se verá a continuación, es un archivo de texto simple en formato ASCII y no existe ningún programa que permita configurarlo de una manera fácil, por lo que el administrador de la red debe ser muy cuidadoso y paciente a la hora de hacerle cambios.

En el archivo existen cinco secciones básicas agrupadas de la siguiente manera:

- Sección de opciones generales
- Sección de direcciones MAC
- Sección de grupos de puertos
- Sección de grupos de VLANs
- Sección de políticas de puertos

El archivo consta de un formato específico con palabras reservadas y cada entrada inicia en una línea nueva. Al comienzo del archivo debe escribirse la palabra “VMPS” para prevenir que el VMPS lea otros tipos de archivos de configuración. Es de destacar que cuando se quiera agregar un comentario a una línea, se debe utiliza el carácter “!” al inicio de ésta (ejemplo: !vmps fallback PRUEBA).

2.4.1. Sección de Opciones Generales

En ésta sección se detallan las opciones generales con las que trabaja el VMPS. La sintaxis de cada comando y su respectiva descripción, se detalla a continuación:

- ***vmps domain <domain-name> :*** Dominio en el que trabajará el VMPS. Los switches clientes deben tener el mismo dominio.
- ***vmps mode { open | secure } :*** Modo de seguridad, si no se especifica trabajará en modo no seguro.
- ***vmps fallback <vlan-name> :*** Si se especifica esta línea, el VMPS enviará este nombre de VLAN cuando la dirección MAC del host no se encuentre en la base de datos. Esta es una VLAN por defecto, pero si no se desea que el host se ingrese a una, se debe escribir --NONE-- .
- ***vmps no-domain-req { allow | deny } :*** Si se especifica “allow”, el VMPS aceptará las peticiones de switches que no tengan el mismo dominio VTP. Si se especifica “deny”, el VMPS sólo aceptará las peticiones de aquellos switches que tienen el mismo dominio VTP del servidor VMPS.

Ejemplo:
En éste ejemplo, se ha configurado un servidor VMPS para que trabaje con el dominio MiVMPS, en modo no seguro, sin VLAN por defecto y que acepte las peticiones de los switches que tengan diferente dominio VTP a MiVMPS.

vmps domain MiVMPS *(dominio)*
vmps mode open *(modo no seguro)*
! vmps fallback PRUEBA *(ésta línea no es leída)*
vmps fallback --NONE-- *(VLAN por defecto)*
vmps no-domain-req allow *(dominio no requerido)*

2.4.2. Sección de Direcciones MAC

En ésta sección se especifica la asignación de dirección MAC a nombre de VLAN. También es posible negar el acceso a una dirección MAC, especificándole que su nombre de VLAN es “--NONE--“, con lo que el VMPS responderá dependiendo del modo de seguridad en el que se encuentre operando.

Sintaxis:

- ***vmps-mac-addrs*** (demarca el inicio de la sección solamente)
- ***address <addr> vlan-name <vlan_name>***

Ejemplos:

- address 0010.a49f.30e1 vlan-name MERCADEO (permite el acceso a la VLAN de MERCADEO)
- address 0010.a49f.30e1 vlan-name --NONE-- (niega el acceso a la dirección MAC)

2.4.3. Sección de Grupos de Puertos

Esta sección permite agrupar puertos de uno o varios switches, para luego aplicarles una política de acceso. Como por ejemplo, se requiere crear una política de acceso para los puertos 1,2,5 del switch A y en todos los puertos del switch B. Esta sección solo define los grupos, las políticas que se aplicarán a estos grupos se hace en la sección de políticas de puertos.

Es posible aplicar las políticas del VMPS a puertos individuales, a grupos de puertos o a todos los puertos de un switch utilizando la palabra reservada **all-ports**. Un puerto es identificado por la dirección IP del switch y el <módulo>/<número de puerto> en la forma de mod_num/port_num.

Sintaxis:

vmps-port-group <group-name>
device <device-id> { port <port-name> | all-ports }

:
:

Ejemplo:
En el siguiente ejemplo, se van a definir dos grupos de puertos. En el primero, se ha especificado el nombre del grupo como Grupo1 y consta del puerto 4 del módulo 2 del switch 10.0.0.1 y de todos los puertos del switch 10.0.0.2 . El segundo grupo, consta del puerto 8 y 10 del switch 10.0.0.15.

vmps-port-group Grupo1
device 10.0.0.1 ***port*** 2/4
device 10.0.0.2 all-ports
vmps-port-group Grupo2
device 10.0.0.15 ***port*** 1/8
device 10.0.0.15 ***port*** 1/10

2.4.4. Sección de Grupos de VLANs

Al igual que la sección de grupos de puertos, esta sección hace posible agrupar VLANs, para luego aplicarles las políticas de acceso en la sección de políticas de puertos.

Sintaxis:
vmps-vlan-group <group-name>
vlan-name <vlan-name>

:
:

Ejemplo:

En el siguiente ejemplo, se crea un grupo de VLANs con el nombre GrupoA y las VLANs son RecursosHumanos y Mercadeo.

vmps-vlan-group GrupoA
vlan-name RecursosHumanos
vlan-name Mercadeo

2.4.5. Sección de Políticas de Puertos

Esta sección hace posible restringir el acceso a las VLANs por medio de los puertos de los switches. Aquí se restringe el acceso a una VLAN o grupo de VLANs, para que puedan ser accedidas solamente desde un puerto de un switch o de un grupo de puertos. Para que lo anterior se pueda llevar a cabo, es necesario que el o los grupos de puertos se hayan definido en la sección de grupos de puertos y que el o los grupos de VLANs se hayan definido en la sección de grupos de VLANs. Si no se especifica ninguna restricción sobre una VLAN, ésta podrá ser accedida desde cualquier puerto dinámico de los switches.

Sintaxis:
vmps-port-policies {vlan-name <vlan_name> | vlan-group <group-name> }
{ port-group <group-name> | device <device-id> port <port-name> }

Ejemplos:

- Este ejemplo, permite el acceso a las VLANs RecursosHumanos y Mercadeo (GrupoA), solamente desde los puertos del Grupo1 (switch 10.0.0.1 puerto 2/4 y todos los puertos del switch 10.0.0.2).
  vmps-port-policies vlan-group GrupoA
  port-group Grupo1

- Este ejemplo, permite el acceso a la Vlan98 solamente a través de los puertos del switch 10.0.0.1.

vmps-port-policies vlan-name Vlan98
device 10.0.0.1 ***port*** all-ports

- El siguiente ejemplo, permite el acceso a la VLAN Finanzas solamente por los puertos que conforman el grupo de puertos GrupoH.
  vmps-port-policies vlan-name Finanzas
  port-group GrupoH

También, es posible aplicar más de una política de acceso a una VLAN o grupo de VLANs, como se demuestra en el siguiente caso:

- Se requiere aplicar una restricción a la VLAN de Mercadeo, para que sea accedida desde todos los puertos del switch 10.0.0.5, desde el puerto 4 del módulo 2 del switch 10.0.0.1 y desde todos los puertos del switch 10.0.0.2.

  Como el grupo de puertos Grupo1 ya cuenta con las últimas 2 restricciones, se puede hacer uso de éste.
  vmps-port-policies vlan-name Mercadeo
  device 10.0.0.5 ***port*** all-ports
  port-group Grupo1

2.5. Puntos principales y comentarios

En general, es importante señalar los siguientes puntos y comentarios sobre el capítulo:

- Los servidores VMPS facilitan la administración de la red, encargándose de la asignación y negación de accesos a las VLANs, una vez que se hayan definido las políticas de membresía.

- Los servidores VMPS ofrecen versatilidad, porque cuando un host es movido de lugar dentro de la red, éste vuelve a pertenecer a la misma VLAN y cuenta con los mismos recursos de red.

- Los servidores VMPS ofrecen la ventaja que están disponibles las 24 horas del día y 365 días del año.

- Con respecto a la seguridad, ésta no se ve afectada por el uso del VMPS, es más, se pueden definir políticas para que ciertos hosts no puedan ingresar a la red.

- Por medio de la sección de políticas de puertos, es posible limitar el acceso a las VLANs, para que sean accedidas solamente por aquellos puertos de switches que se requieran.

- El archivo de configuración podría ser difícil de modificar en redes que cuentan con muchos hosts.

CAPITULO III

3. EL PROTOCOLO DE CONSULTA DE VLANS (VQP)

3.1. Introducción

Este capítulo contiene en detalle, la investigación realizada acerca del protocolo VQP. Se describe la forma en que se transporta a través de la red, los tipos de mensajes que existen y la estructura de las tramas. Además, se presentan algunos ejemplos para ayudar a comprender y utilizar este protocolo que es propietario de CISCO Systems.

La estructura de los mensajes VQP que se presenta, ha sido deducida en base a la captura y análisis de paquetes, entre un VMPS y varios switches. Posteriormente, se desarrollaron diversas simulaciones para comprobar el correcto funcionamiento de los mensajes VQP creados.

3.2. El protocolo VQP es encapsulado por el protocolo UDP

El protocolo de capa de aplicación VQP está encapsulado por UDP en la capa de transporte. Como resultado, el VQP está sujeto a ciertas ventajas y desventajas que el UDP posee. Por ejemplo, el UDP es un protocolo simple, no orientado a conexión en el que no se establecen sesiones. El UDP es comparable al correo convencional, ya que solamente se envía la correspondencia sin necesidad de aviso previo para establecer un canal de comunicación, ni la finalización del mismo. Se contrasta con el protocolo TCP, que es un protocolo orientado a conexión.

El TCP es parecido a una llamada telefónica en la que se establece un canal de comunicación, existe un saludo inicial que inicia la conversación y una despedida que finaliza el vínculo de comunicación. El UDP es un protocolo de máximo esfuerzo, descrito como no confiable ya que no maneja acuses de recibo y no garantiza que los paquetes lleguen a su destino. Una de las ventajas del UDP es que permite la

transferencia de datos entre hosts de forma rápida, al tener un costo de operación menor que su contraparte, el TCP. El UDP es el protocolo de preferencia para transmitir cantidades pequeñas de datos, donde es mayor el costo operativo del establecimiento de sesiones y verificación de datos que una simple retransmisión de la información necesaria. Por lo tanto el UDP es el protocolo que mejor cubre las necesidades del modelo de aplicación petición-respuesta del VMPS. En este caso, la respuesta del servidor VMPS sirve como una confirmación de recepción de la consulta realizada por el cliente. Si el cliente no recibe la respuesta en un período de tiempo determinado, simplemente se retransmite la petición.

El protocolo VQP no cuenta con seguridad alguna, por lo que hay que tener cuidado en la forma de la implementación de las VLANs dinámicas. Si se desea algún tipo de seguridad en el uso del VQP, habrá que implementarlo a nivel del software (capa de aplicación).

3.3. Los mensajes VQP

La comunicación entre el switch cliente y el VMPS se inicia cuando el switch necesita obtener el nombre de la VLAN a la que debe configurar un puerto cuando un nuevo host desea ingresar a la red, o cuando necesita reconfirmar el nombre de la VLAN a la que un puerto ya tiene acceso. Esta comunicación se lleva a cabo por medio de mensajes, los cuales se pueden agrupar de la siguiente manera:

- Mensajes de peticiones
- Mensajes de respuestas.
- Mensajes de respuestas de error.

Los mensajes de peticiones están conformados por dos tipos: solicitud de VLAN y reconfirmación. El primero, es el mensaje de solicitud del nombre de la VLAN que debe asignarle a un puerto, cuando un nuevo host que está tratando de ingresar a la red por dicho puerto. El segundo es el mensaje de reconfirmación, el cual los switches envían en intervalos de tiempo que se les ha configurado, para reconfirmar

el nombre de la VLAN que se le ha asignado al puerto en donde se encuentra un host activo.

Los mensajes de respuestas son las respuestas que el VMPS envía al switch con la información solicitada previamente por las peticiones. Por cada mensaje de petición, hay un mensaje de respuesta. El VMPS puede responder con un mensaje de acceso concedido a una VLAN o con un acceso denegado. Dependiendo del modo de funcionamiento del VMPS, el acceso denegado puede ser de dos tipos, los cuales se detallan a continuación:

- ***Permiso denegado.*** El VMPS está operando en modo no seguro y el host no tiene permiso de acceder a la red.
- ***Permiso denegado, deshabilitar puerto.*** El VMPS está operando en modo seguro y el host no tiene permiso de acceder a la red. El switch debe deshabilitar su puerto.

Los mensajes de respuestas de error, también son respuestas a las peticiones del switch. Sin embargo, a diferencia de los mensajes de respuesta, el VMPS ha determinado en base al mensaje que el switch le envió, que no puede darle ingreso a la red al host por algún dato que se encuentra en el encabezado del mensaje. Algunos de estos mensajes le indican al switch que debe tomar una acción.

A continuación se listan los mensajes de error que el VMPS envía al switch:

- ***Error de versión de protocolo.*** El mensaje que recibió el VMPS, tiene una versión de protocolo no soportada.
- ***No hay recursos.*** El VMPS no tiene los suficientes recursos para procesar la petición.
- ***Dominio incorrecto.*** El dominio del switch no concuerda con el del VMPS.

Cada uno de estos mensajes tiene un formato específico y su longitud varía. Por medio de la captura de mensajes en la red, se ha logrado identificar las estructuras de cada uno de ellos.

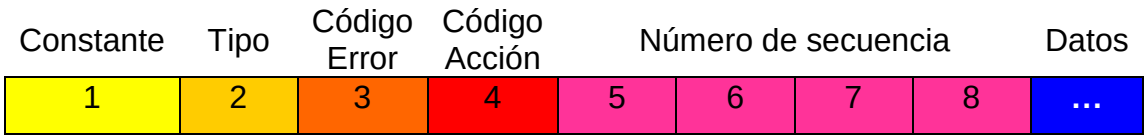
3.4. Estructura del mensaje VQP

A partir de la captura de los mensajes que fluyen en la red entre un switch y un VMPS, se puede concluir que la estructura del paquete VQP cumple con las siguientes condiciones:

- Los mensajes VQP están divididos en dos partes, el encabezado y los datos.
- Los mensajes de error o negación al acceso, solo poseen encabezado.
- El encabezado consta de 8 bytes y se encuentra subdividido de la siguiente manera:

Byte	Descripción
1	Permanece constante en todos los mensajes, posiblemente indica la versión del protocolo.
2	Tipo de mensaje
3	Códigos de error
4	Códigos de acción
5 al 8	Número de secuencia del mensaje

Tabla 2. Estructura del encabezado VQP.



- La sección de los datos en el mensaje es variable y está conformado de la siguiente manera para cada dato:

    - 4 bytes indicando el tipo de dato que viene a continuación.
    - 2 bytes indicando la longitud del dato.
    - El dato.

Tipo de dato				Longitud del dato que sigue a continuación		Dato			
Hx00	Hx00	Hx0C	Hx01	Hx00	Hx04	HxC0	HxA8	Hx03	Hx96

- Los posibles valores para los bytes de descripción de los mensajes son los siguientes:

ENCABEZADO	
Byte	**Valores posibles**
1	Constante
2	Hx01 Petición de acceso a la red Hx02 Respuesta a la petición de acceso Hx03 Petición de confirmación Hx04 Respuesta de petición de confirmación
3	Hx00 No hay error Hx01 Error de versión de protocolo Hx02 No hay recursos Hx03 Permiso denegado. (Modo no seguro) Hx04 Permiso denegado, deshabilitar puerto. (Modo seguro) Hx05 Dominio incorrecto.
4	Hx00 Mensaje de error Hx02 Contestación con el nombre de la VLAN Hx05 Petición sin dominio configurado en el switch cliente Hx06 Petición con dominio configurado en el switch cliente
5 al 8	Número de secuencia del mensaje. Este valor es diferente para cada mensaje. Es calculado por el switch y el VMPS debe responder con el mismo valor.

Tabla 3. Valores posibles para el encabezado de los mensajes VQP.

DATOS	
Tipos de datos (hexa)	**Descripción**
00 00 0C 01	IP del switch
00 00 0C 02	Número del puerto
00 00 0C 03	Nombre de la VLAN
00 00 0C 04	Nombre del dominio
00 00 0C 05	(Desconocido)
00 00 0C 06	Dirección MAC (Para peticiones)
00 00 0C 07	Constante en cero en todas las pruebas
00 00 0C 08	Dirección MAC (Para respuestas)

Tabla 4. Tipos de datos en los mensajes VQP.

3.5. Ejemplos

3. *Mensaje de petición por parte del switch al VMPS, cuando el switch necesita obtener el nombre de la VLAN para el puerto.*

Hexadecimal	ASCII
01 01 00 06 15 00 00 00 **00 00 0c 01** *00 04* c0 a8 03 96 **00 00 0c 02** *00 02* 31 30 **00 00 0c 03** *00 08* 2d 2d 4e 4f 4e 45 2d 2d **00 00 0c 04** *00 07* 4b 52 59 50 54 4f 53 **00 00 0c 07** *00 01* 00 **00 00 0c 06** *00 06* 00 02 2d 1a a0 9e	....10...... --NONE--......KR YPTOS........... ....-...

Encabezado:

01 = Constante

01 = Petición de acceso a la red

00 = No hay error

06 = Es una petición

15 00 00 00 = Número de secuencia

Datos:

00 00 0c 01 = Continua la IP del switch

00 04 = Posee 4 bytes c0 a8 03 96 = 192.168.3.150 = IP del switch
00 00 0c 02 = Continúa el número del puerto *00 02* = Posee 2 bytes 31 30 = 10 (en ASCII #31 = 1, #30 = 0)
00 00 0c 03 = Continúa el nombre de la VLAN *00 08* = Posee 8 bytes 2d 2d 4e 4f 4e 45 2d 2d = --NONE-- (en ASCII)
00 00 0c 04 = Continúa el nombre de dominio *00 07* = Posee 7 bytes 4b 52 59 50 54 4f 53 = KRYPTOS (en ASCII)
00 00 0c 07 = Continúa una constante en cero? *00 01* = Posee 1 byte 00 = 0
00 00 0c 06 = Continúa la dirección MAC del dispositivo *00 06* = Posee 6 bytes 00 02 2d 1a a0 9e = 00-02-2d-1a-a0-9e

4. *Mensaje de respuesta por parte del VMPS, en donde le envía al switch la VLAN a la que debe configurar el puerto.*

Hexadecimal	ASCII
01 02 00 02 15 00 00 00 **00 00 0c 03** *00 06* 50 52 55 45 42 41 **00 00 0c 08** *00 06* 00 02 2d 1a a0 9e	..............PR UEBA........-...

Encabezado:

01 = Constante

02 = Respuesta a la petición de acceso

00 = No hay error

02 = Contestación con el nombre de la VLAN

15 00 00 00 = Número de secuencia

Datos:

00 00 0c 03 = Continúa el nombre de la VLAN *00 06* = Posee 6 bytes 50 52 55 45 42 41 = PRUEBA (en ASCII)
00 00 0c 08 = Continúa la dirección MAC del dispositivo *00 06* = Posee 6 bytes 00 02 2d 1a a0 9e = 00-02-2d-1a-a0-9e

5. *Mensaje de respuesta por parte del VMPS, en donde se niega el acceso a la red. El VMPS está trabajando en modo no seguro:*

Hexadecimal	ASCII
01 02 03 00 15 00 00 00	.....

Encabezado:

01 = Constante

02 = Respuesta a la petición de acceso

03 = Acceso denegado

00 = Hay error

15 00 00 00 = Número de secuencia

6. *Mensaje de respuesta por parte del VMPS, en donde se niega el acceso a la red. El VMPS está trabajando en modo seguro:*

Hexadecimal	ASCII
01 02 04 00 15 00 00 00	.....

Encabezado:

01 = Constante

02 = Respuesta a la petición de acceso

04 = Acceso denegado, deshabilitar el puerto

00 = Hay error

15 00 00 00 = Número de secuencia

3.6. Puntos principales y comentarios

Lo más importante que se puede destacar de éste capítulo, son los siguientes puntos:

- El protocolo VQP consta de mensajes que pueden ser subdivididos en tres categorías: mensajes de peticiones, mensajes de respuestas, mensajes de respuestas de error.

- Los mensajes VQP son encapsulados por el protocolo UDP, para ser transportados en la red.

- Los mensajes VPQ están conformados por una sección de encabezado y una de datos.

- Los mensajes VQP viajan en la red sin ningún tipo de encripción, por lo que se sugiere que se adopten medidas de seguridad adecuadas en el acceso a la VLAN utilizada por el VMPS, si se desea implementar éste protocolo.

- Es posible crear un programa VMPS utilizando la estructura del VQP descrita en éste capítulo, para generar mensajes de respuesta a las peticiones de switches trabajando con puertos dinámicos.

- También, es posible incorporar este protocolo a otros programas, tales como programas estadísticos de red, sniffers, etc.

CAPITULO IV

4. DESARROLLO DEL SERVIDOR VMPS

4.1. Introducción

En este capítulo, se explica el funcionamiento de un servidor VMPS que se ha desarrollado para demostrar el uso de las VLANs dinámicas. Para tal propósito, se han utilizado diagramas de flujo de datos (DFD), los cuales permiten esquematizar y explicar el funcionamiento de un sistema. Además, se muestra el diagrama E-R de la base de datos que utiliza el programa, con su respectivo diccionario de datos.

4.2. El Free VMPS

Free VMPS es un servidor VMPS que se ha desarrollado para demostrar el uso de las VLANs dinámicas y confirmar la estructura del protocolo VQP. Sin embargo no se limita a eso, porque puede ser utilizado en una empresa, centro educativo, etc. de forma gratuita para manejar sus VLANs dinámicas.

Al Free VMPS se le ha realizado una variante con respecto a los servidores VMPS normales. El archivo de configuración se ha cambiado por una base de datos, por lo que, con un software diseñado para configurarla se facilita la administración los hosts, VLANs y permisos sobre éstas.

También, se le han desarrollado dos herramientas que ayudarán a los administradores de red en sus actividades diarias. La primera, es un programa que permite administrar la base de datos de los hosts, VLANs y permisos de VLANs desde la Web. Tiene la ventaja que posee una interfaz gráfica accesible desde cualquier navegador. Además, ayuda a reducir los tiempos y a detectar errores en la administración de las VLANs dinámicas.

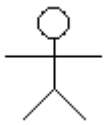
La segunda herramienta es el Inspector de Redes. Es una herramienta que tiene como objetivo, inspeccionar un una o un rango de IP's de la red y generar un archivo con la dirección MAC, IP y nombre de los hosts encontrados. Este programa facilita la inserción de la información anterior en la base de datos , cuando se quiere cambiar de una red plana a una con VLANs dinámicas. Este archivo puede ser importado por el programa de administración de la base de datos e ingresar toda la información de un solo en sus tablas. Definitivamente, ahorraría varias horas de trabajo cuando no se cuenta con esa información.

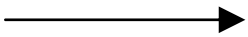
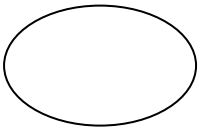
4.3. Modelo de caso de uso del Free VMPS

Son una herramienta UML (Lenguaje Unificado de Modelado), que ayuda a los diseñadores de software a describir el funcionamiento un sistema, dejando a un lado en como éste lo hace. Su propósito, es el de enfocarse en lo que el sistema debe hacer, en vez de cómo lo debe hacer; el de contar la historia en como el actor logra obtener algo del sistema. Estos pueden ser representados por diagramas, pero principalmente son descritos en texto. Además, debe tomarse en cuenta, que no son utilizados para analizar requerimientos o descomponerlos en partes más pequeñas.

Los modelos de caso de usos, son el conjunto de actores y casos de uso que describen el funcionamiento de un sistema.

4.3.1. Convenciones utilizadas

 Actor	Representa una persona, programa, máquina o cualquier cosa que de alguna manera interactúa con el sistema. Por definición, estos se encuentran fuera del sistema.

Relaciones 	Conecta a los actores y los casos de uso con los que interactúan. La cabeza de la flecha, indica quien inicia la interacción.
 Caso de Uso	Representa las cosas que el sistema debe realizar a petición de los actores. Los casos de uso no son funciones y no pueden ser descompuestos.

4.3.2. Catálogo de actores

La Figura 10. muestra todos los actores en el modelo de caso de uso del Free VMPS. Se da una breve descripción de los actores después de la figura.

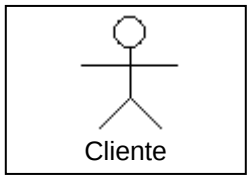


Figura 10. Actor del Free VMPS.

- **Cliente:** El Cliente representa a un switch. Este permite o niega el acceso a la red a los dispositivos que se conectan en sus puertos. Cuando se conecta o activa un host en uno de sus puertos configurado como dinámico, consulta al sistema para obtener el nombre de VLAN al que debe configurar su puerto. También consulta al sistema, cuando el intervalo de tiempo para las reconfirmaciones de las VLANs ha sido alcanzado.

4.3.3. Catálogo de casos de uso

4.3.3.1. Caso de uso primario

La Figura 11. muestra el modelo principal de caso de uso del Free VMPS.

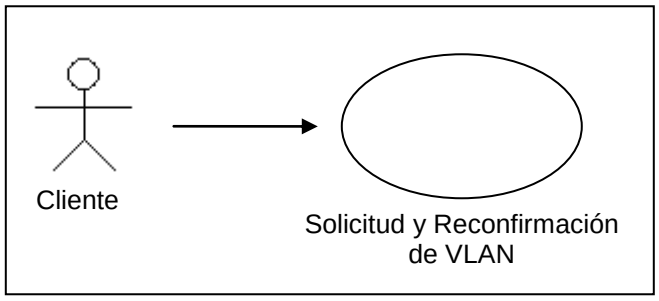


Figura 11. Caso de uso primario del Free VMPS.

Solicitud y Reconfirmación de VLAN: Este caso de uso describe como el sistema procesa la petición del switch Cliente, al momento que éste le solicita el nombre de VLAN a la que el puerto debe configurarse, cuando un nuevo host se ha conectado o activado en el puerto. También, cuando el switch Cliente le está reconfirmando el nombre de VLAN al que el puerto se encuentra configurado.

4.3.3.2. Caso de uso "Solicitud y Reconfirmación de VLAN"

1. *Precondiciones*
   - El VMPS debe ser configurado antes de que los puertos se configuren como dinámicos.
   - El dominio de administración VTP de los clientes del VMPS y el del servidor VMPS debe ser el mismo.
   - La VLAN de administración de los clientes del VMPS y el del servidor VMPS debe ser la misma.
   - El Cliente debe tener configurado los puertos como dinámicos y la dirección IP del servidor VMPS.
   - La conexión de red entre el servidor VMPS y el Cliente debe estar activa.
   - Ya debe existir en la base de datos la información de los clientes, hosts, grupos de puertos, grupos de VLANs y las políticas de puertos.

2. *Flujo básico*

   { Recibir petición }

1. El caso de uso comienza cuando el actor Cliente envía un mensaje VQP por el puerto 1589, con la información del host que desea ingresar a la red por uno de sus puertos y la suya. La información que envía es la dirección IP, dominio y puerto del Cliente, y la dirección MAC del host.

{ Guardar en Bitácora Información Recibida }

2. El sistema guarda en bitácora la información recibida.

{ Verificar Versión Mensaje }

3. El sistema verifica si la versión del mensaje es soportada.

{ Autenticar Cliente }

4. El sistema compara el dominio del cliente con el suyo.

{ Obtener VLAN }

5. El sistema busca la dirección MAC del host y determina la VLAN asignada. Si la VLAN está restringida, verifica si la VLAN está permitida en el Cliente para dicho puerto.

{ Devolver VLAN }

6. El sistema envía un mensaje VQP al Cliente con el nombre de la VLAN a la que debe configurar el puerto.

{ Guardar en Bitácora Información Enviada }

7. El sistema guarda en bitácora la información enviada.

{ Caso de uso termina }

8. El caso de uso termina.

3. *Flujos alternativos*

3.1. Error en mensaje recibido

Inicia en **{ Recibir petición }**.

1. Si el mensaje recibido no cumple con la estructura establecida, entonces ignorarlo.
2. Retorna al flujo básico en **{ Caso de uso termina }**.

3.2. Error en versión de mensaje VQP

Inicia en **{ Verificar Versión Mensaje }**.

1. Si la versión del mensaje VQP recibida no es soportada por el VMPS, entonces, enviar un mensaje al Cliente de error en la versión del mensaje VQP.
2. Retorna al flujo básico en **{ Guardar en Bitácora Información Enviada }**.

3.3. Fallo en la autenticación del Cliente

Inicia en **{ Autenticar Cliente }**.

1. Si el sistema requiere que el dominio del Cliente sea igual al suyo y no lo es, entonces, enviar un mensaje al Cliente que el dominio no es correcto.
2. Retorna al flujo básico en **{ Guardar en Bitácora Información Enviada }**.

3.4. No se encuentra al host

Inicia en **{ Obtener VLAN }**.

1. Si no se encuentra la dirección MAC del host en la base de datos, entonces, ***responder por modo de funcionamiento***.
2. Retorna al flujo básico en **{ Guardar en Bitácora Información Enviada }**.

3.5. VLAN no permitida en el puerto

Inicia en **{ Obtener VLAN }**.

1. Si la VLAN está restringida y no está permitida en dicho puerto, entonces, ***responder por modo de funcionamiento***.
2. Retorna al flujo básico en **{ Guardar en Bitácora Información Enviada }**.

3.6. Error en el sistema

3.6.1 Error al procesar la solicitud

1. Si en cualquier punto del uso de caso hay un error interno en el sistema, entonces, retornar al flujo básico en **{ Caso de uso termina }**

3.6.2 Error al guardar en bitácora

Si en cualquier punto del uso de caso no se puede guardar en la bitácora, entonces, el sistema hace lo siguiente:

1. El sistema mostrará un mensaje en pantalla.
2. Retornar al flujo básico en **{ Caso de uso termina }**.

4. Subflujos

1. Responder por modo de funcionamiento

a. Si el sistema trabaja en modo seguro, entonces enviar un mensaje al Cliente que debe deshabilitar el puerto.
b. Si el sistema trabaja en modo no seguro:
   - Si tiene configurado una VLAN por defecto, entonces enviar un mensaje al Cliente con el nombre de la VLAN por defecto.
   - Si no tiene configurado una VLAN por defecto, entonces enviar un mensaje al Cliente con el nombre de VLAN “--NONE--“.

5. Poscondiciones

Ningunas

6. Requerimientos especiales

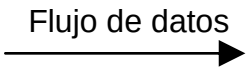
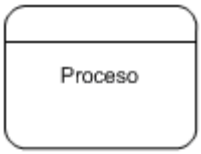
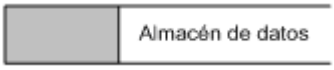
Ningunos

4.4. Diagramas de flujos de datos (DFD)

Por medio de los diagramas de flujos de datos (DFD), es posible representar gráficamente el funcionamiento lógico de un sistema y cuales son las

transformaciones que sufren los datos a medida que pasan por sus procesos. Esta herramienta permite dar una idea general y luego profundizar en cada uno de los componentes del sistema hasta el nivel deseado, y así, comprender como trabaja el sistema.

4.4.1. Convenciones utilizadas

	Representa una persona, programa, máquina o cualquier cosa que de alguna manera interactúa con el sistema. Por definición, estos se encuentran fuera del sistema.
	Representa la introducción de datos en un proceso o la obtención de datos de un proceso.
	Representa un conjunto de tareas o acciones realizadas a partir de un flujo de datos de entrada para producir flujos de datos de salida.
	Representa algunos lugares en donde se guarda la información temporalmente o permanentemente.

4.4.2. Desarrollo de los DFD's del Free VMPS

4.4.2.1. Diagrama de contexto

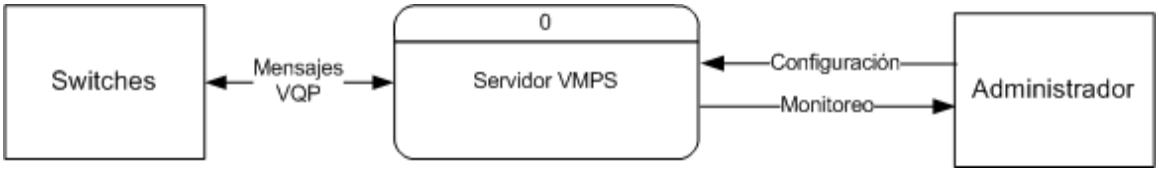


Figura 12. Diagrama a nivel de contexto del VMPS

En la Figura 12. se muestran las entidades con las que el sistema interactúa.

Como se puede apreciar en el diagrama, el servidor VMPS genera mensajes de respuesta (mensajes VQP) a las peticiones de los switches; además, permite que el administrador pueda configurarlo y monitorear su funcionamiento.

4.4.2.2. Diagrama de contexto nivel 0

En la Figura 13. se pueden observar los distintos componentes a nivel general que integran al servidor VMPS, los cuales se detallan a continuación:

1. *Procesador de Mensajes VQP:* Este componente es el encargado del manejo de los mensajes VQP. Recibe, interpreta, valida, consulta, genera y envía los mensajes VQP a los switches clientes que lo solicitan.
2. *Servidor Http:* Este componente provee la interfaz del sistema en páginas HTML, por el cual el usuario (administrador del VMPS) puede configurar y monitorear el funcionamiento del VMPS.
3. *Generador de Bitácora:* Este componente recibe todos los eventos del sistema (errores, mensajes del sistema, estatus del servidor, etc) y los registra en el archivo de bitácora.
4. *Módulo de configuración:* Este componente se encarga de leer, retener en memoria y escribir todos los parámetros de configuración para el correcto funcionamiento del sistema.

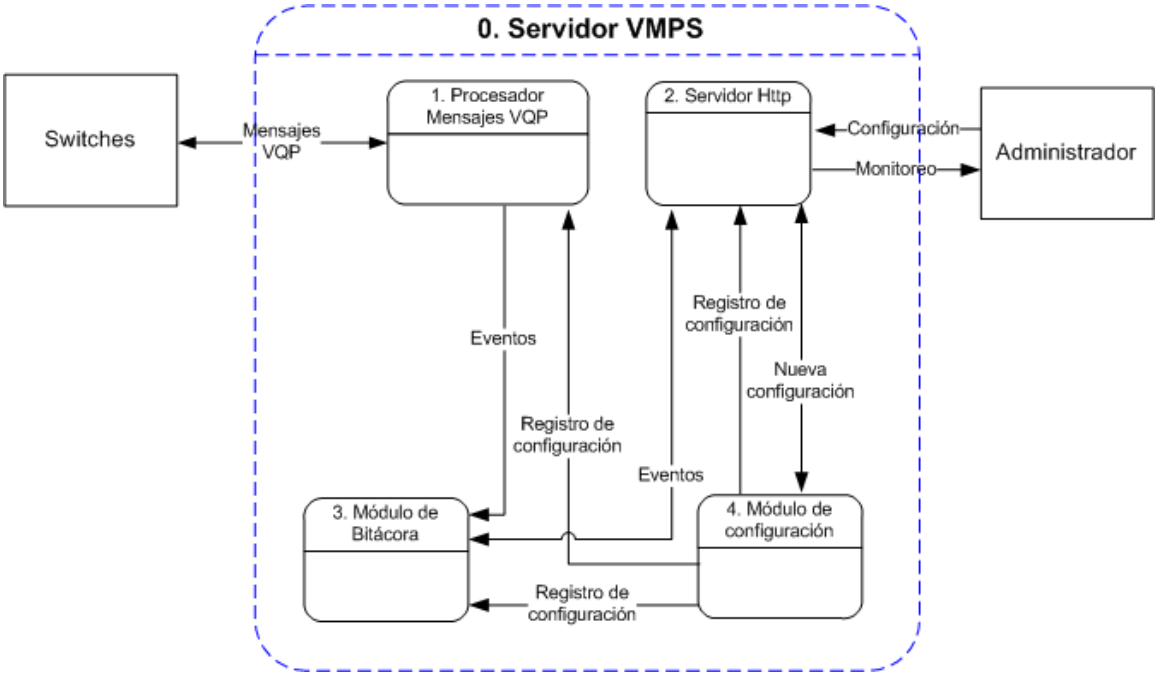


Figura 13. Diagrama de contexto nivel 0 del VMPS

4.4.2.3. Diagrama del Procesador de Mensajes VQP

El diagrama de la Figura 14. permite distinguir el proceso que sigue el Procesador de Mensajes VQP cuando recibe un mensaje de un switch y las opciones que influyen en la toma de decisiones para generar el mensaje de respuesta.

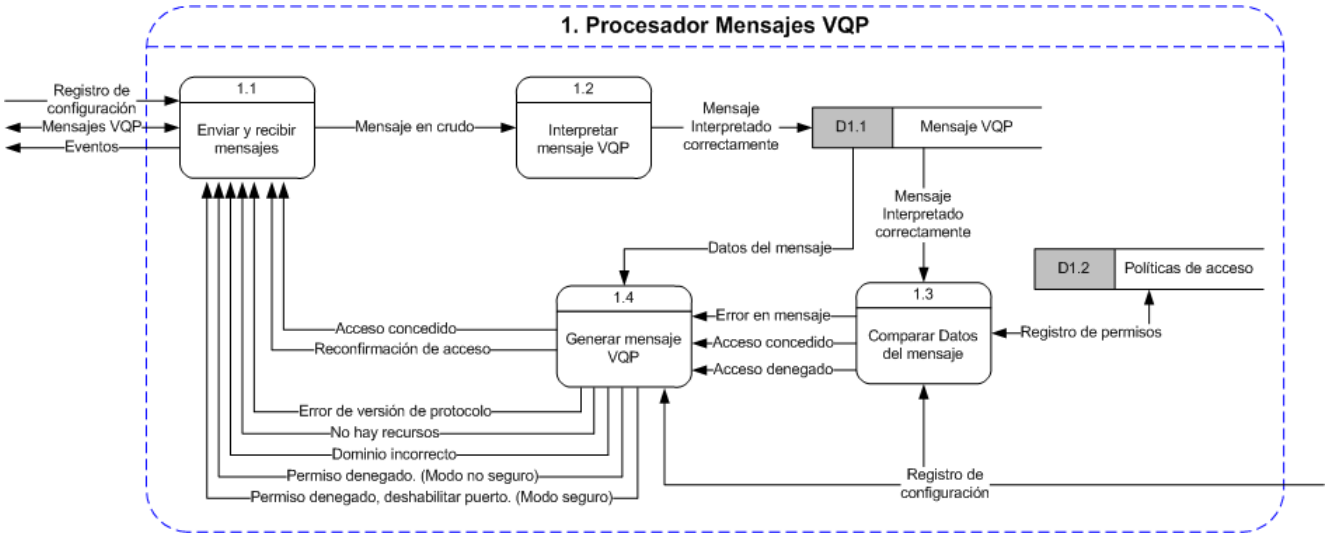


Figura 14. Diagrama del Procesador de Mensajes VQP

Descripción de los procesos:

No.	Proceso	Descripción
1.1	Enviar y recibir mensajes	Este proceso utiliza un componente UDP para la recepción y envío de mensajes VQP sobre la red. Cuando este componente recibe un mensaje VQP (encapsulado en UDP), lo desempaqueta y lo pasa al paso 1.2 . Cuando el paso 1.4 le manda el mensaje VQP a enviar, este lo encapsula y lo envía al switch cliente. Para que este componente funcione, debe leer su registro de configuración del Módulo de Configuración. Cuando recibe o envía algún mensaje, éste envía el evento al componente de bitácoras para que lo registre.
1.2	Interpretar mensaje VQP	En este paso, al mensaje en “crudo” se le trata de extraer cada uno de los campos del mensaje VQP. Si el mensaje no sigue la estructura definida de los mensajes VQP, es desechado y no continúa al paso 1.3 . Si el mensaje se pudo interpretar, es guardado en memoria.
1.3	Comparar datos del mensaje	Del mensaje se utilizan la dirección MAC del host, IP del switch, puerto VLAN, dominio del switch y se buscan y comparan con las políticas de acceso. Dependiendo de la comparación de la información encontrada y los parámetros de configuración, se decide que tipo de mensaje se debe enviar.
1.4	Generar mensaje VQP	Con los datos encontrados en el paso anterior, el tipo de mensaje, el mensaje VQP interpretado y el registro de configuración, se crea un mensaje VQP para ser enviado de respuesta al switch cliente por medio del paso 1.1 .
D1.1	Mensaje VQP	Es un registro que contiene los diferentes campos que contiene el mensaje VQP que se ha recibido en ese momento.
D1.2	Políticas de acceso	Es un base de datos en donde se encuentran asociados los hosts con las VLANs respectivas y los permisos con los que cuenta en los puertos de los switches.

4.4.2.4. Diagrama del Procesador de Mensajes VQP

La Figura 15. muestra como esta conformado el Módulo de Bitácora.

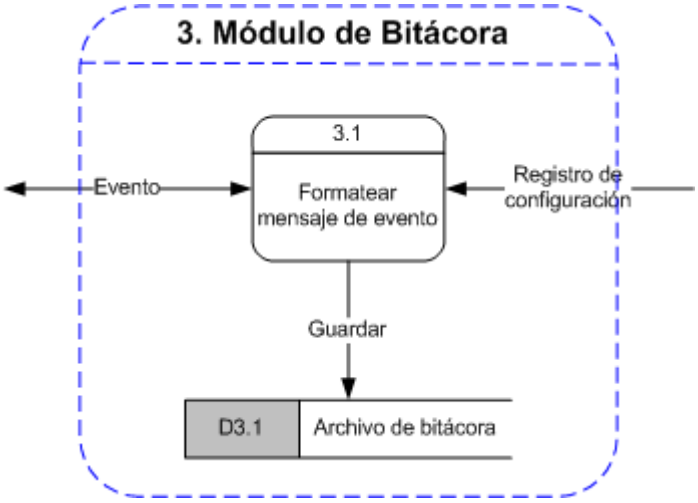


Figura 15. Diagrama del Módulo de Bitácora

Descripción de los procesos:

No.	Proceso	Descripción
3.1	Formatear mensaje de evento	Cuando recibe algún evento (mensaje del sistema, mensaje de error, etc), éste le añade la fecha y hora y lo guarda en un archivo de texto. En el registro de configuración se define si el mensaje debe ser guardado o no. A continuación, le manda el mismo mensaje al Servidor http para que lo muestre en la página de monitoreo.
D3.1	Archivo de bitácora	Este es un archivo de texto el cual cumple el estándar W3C para archivos de bitácoras.

4.4.2.5. Diagrama del Módulo de Configuración

La Figura 16. muestra como esta conformado el Módulo de Configuración.

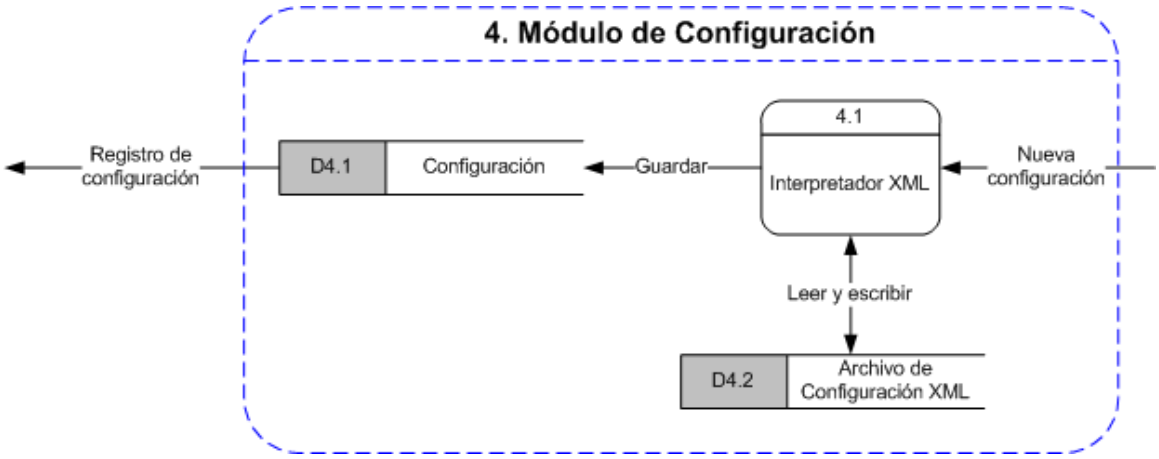


Figura 16. Diagrama del Módulo de Configuración

Descripción de los procesos:

No.	Proceso	Descripción
4.1	Interpretador XML	Cuando el interpretador XML recibe una nueva configuración por parte del Servidor Http, la guarda en un archivo de configuración en formato XML. Cuando se le pide leer la configuración, éste lo extrae del archivo y la guarda en memoria para que los demás componentes del sistema tengan acceso a ella cuando lo necesiten.
D4.1	Configuración	Es un registro en memoria que contiene toda la información leída del archivo de configuración XML
D4.2	Archivo de Configuración XML	Es un archivo en formato XML que contiene la configuración del VMPS. Este, utiliza la versión 1.0 y el tipo de codificación ISO8859-1 según los estándares para archivos XML.

4.5. Base de datos

4.5.1. Diagrama Entidad – Relación (E – R)

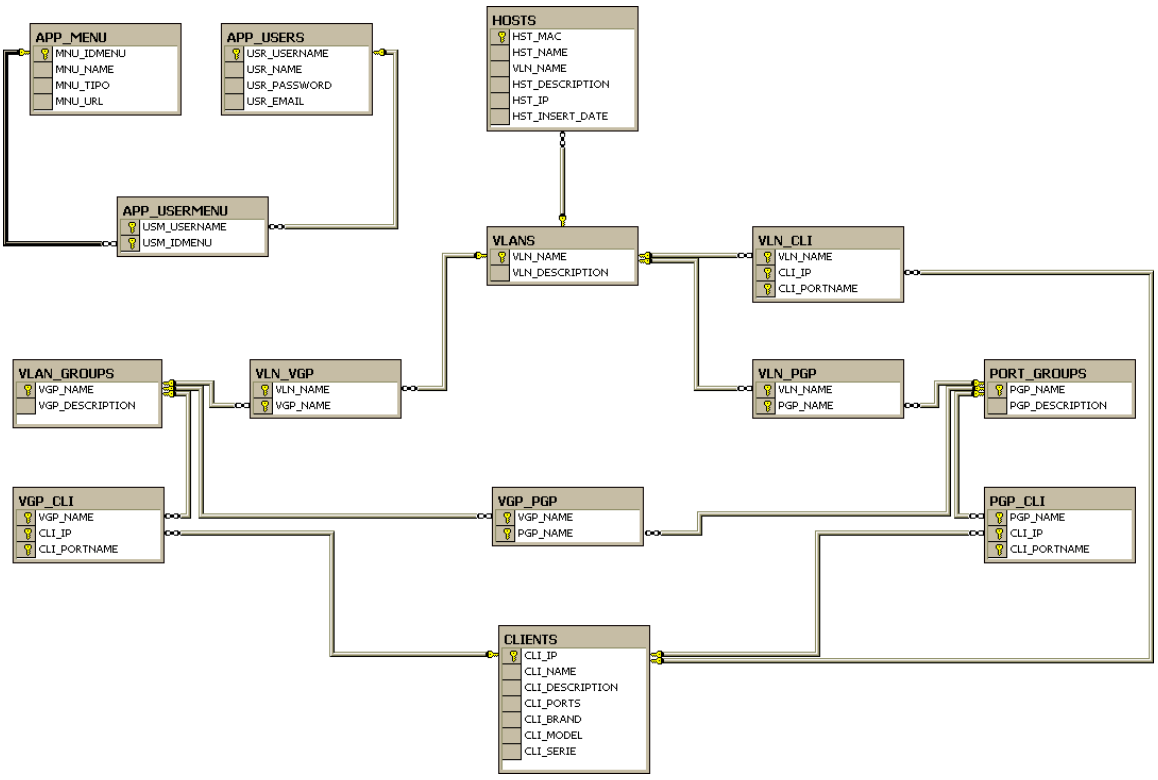


Figura 17. Ejemplo Diagrama E-R del Servidor VMPS.

4.5.2. Descripción de Tablas

4.5.2.1. Tabla APP_MENU

Descripción: Tabla que contiene el menú para el programa Web de configuración de la base de datos.

Campo	Tipo	Longitud	Nulo
MNU_IDMENU	int		
MNU_NAME	varchar	50	
MNU_TIPO	int		
MNU_URL	varchar	50	

Llaves primarias:

- VLN_NAME (autoincremental)

4.5.2.2. Tabla APP_USERS

Descripción: Tabla que contiene a los usuarios que acceden al programa Web de configuración de la base de datos.

Campo	Tipo	Longitud	Nulo
USR_USERNAME	varchar	30	
USR_NAME	varchar	40	
USR_PASSWORD	varchar	59	
USR_EMAIL	varchar	50	✔

Llaves primarias:

- VLN_NAME (autoincremental)

4.5.2.3. Tabla APP_USERMENU

Descripción: Tabla que relaciona los menús con cada usuario. Indica a que opciones del menú tiene acceso cada usuario.

Campo	Tipo	Longitud	Nulo
USM_USERNAME	varchar	30	
USM_IDMENU	int		

Llaves primarias:

- USM_USERNAME, USM_IDMENU

Llaves foráneas:

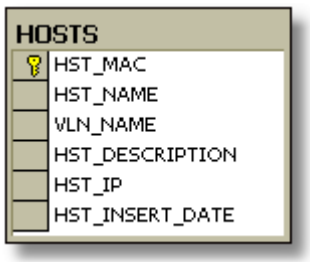
- FK_APP_USERMENU_APP_USERS

Tabla llave Primaria	Campos	Tabla llave Foránea	Campos
APP_USERS	USR_USERNAME	APP_USERMENU	USM_USERNAME

- FK_APP_USERMENU_APP_MENU

Tabla llave Primaria	Campos	Tabla llave Foránea	Campos
APP_MENU	MNU_IDMENU	APP_USERMENU	USM_IDMENU

4.5.2.4. Tabla HOSTS



Descripción: Tabla principal de los hosts.

Campo	Tipo	Longitud	Nulo
HST_MAC	varchar	17	
HST_NAME	varchar	50	
VLN_NAME	varchar	30	
HST_DESCRIPTION	varchar	50	✓
HST_IP	varchar	15	✓
HST_INSERT_DATE	datetime	8	

Llaves primarias:

- HST_MAC

Llaves foráneas:

- FK_HOSTS_VLANS

Tabla llave Primaria	Campos	Tabla llave Foránea	Campos
VLANS	VLN_NAME	HOSTS	VLN_NAME

4.5.2.5. Tabla VLANs

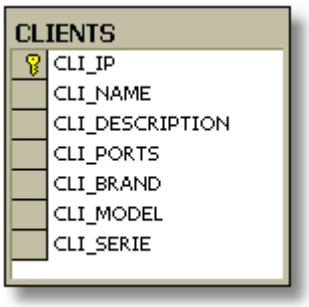
Descripción: Tabla principal de las VLANs

Campo	Tipo	Longitud	Nulo
VLN_NAME	varchar	30	
VLN_DESCRIPTION	varchar	50	✓

Llaves primarias:

- VLN_NAME

4.5.2.6. Tabla CLIENTS



Descripción: Tabla principal de los switches clientes.

Campo	Tipo	Longitud	Nulo
CLI_IP	varchar	15	
CLI_NAME	varchar	15	
CLI_DESCRIPTION	varchar	50	✓
CLI_PORTS	int		✓
CLI_BRAND	varchar	25	✓
CLI_MODEL	varchar	25	✓
CLI_SERIE	varchar	25	✓
CLI_SNMPRO	varchar	15	
CLI_SNMPWR	varchar	15	

Llaves primarias:

- CLI_IP

4.5.2.7. Tabla PORT_GROUPS

Descripción: Tabla principal de los grupos de puertos.

Campo	Tipo	Longitud	Nulo
PGP_NAME	varchar	30	
PGP_DESCRIPTION	varchar	50	✓

Llaves primarias:

- PGP_NAME

4.5.2.8. Tabla VLAN_GROUPS

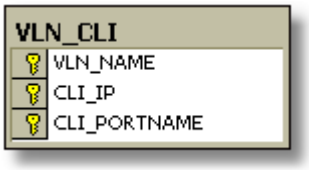
Descripción: Tabla principal de los grupos de VLANs.

Campo	Tipo	Longitud	Nulo
VGP_NAME	varchar	30	
VGP_DESCRIPTION	varchar	50	✓

Llaves primarias:

- VGP_NAME

4.5.2.9. Tabla VLN_CLI



Descripción: Esta tabla permite definirle a las VLANs los puertos de los switches a los que tendrán permiso.

Campo	Tipo	Longitud	Nulo
VLN_NAME	varchar	30	
CLI_IP	varchar	15	
CLI_PORTNAME	varchar	10	

Llaves primarias:

- VLN_NAME, CLI_IP, CLI_PORTNAME

Llaves foráneas:

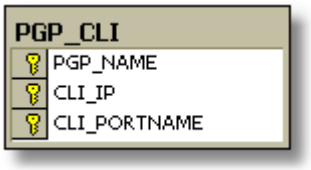
- FK_VLN_CLI_VLANS

Tabla llave Primaria	Campos	Tabla llave Foránea	Campos
VLANS	VLN_NAME	VLN_CLI	VLN_NAME

- FK_VLN_CLI_CLIENTS

Tabla llave Primaria	Campos	Tabla llave Foránea	Campos
CLIENTS	CLI_IP	VLN_CLI	CLI_IP

4.5.2.10. Tabla PGP_CLI



Descripción: Esta tabla permite definirle a los grupos de puertos los puertos de los switches a los que tendrán permiso.

Campo	Tipo	Longitud	Nulo
PGP_NAME	varchar	30	
CLI_IP	varchar	15	
CLI_PORTNAME	varchar	10	

Llaves primarias:

- PGP_NAME, CLI_IP, CLI_PORTNAME

Llaves foráneas:

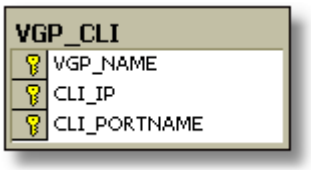
- FK_PGP_CLI_PORT_GROUPS

Tabla llave Primaria	Campos	Tabla llave Foránea	Campos
PORT_GROUPS	PGP_NAME	PGP_CLI	PGP_NAME

- FK_PGP_CLI_CLIENTS

Tabla llave Primaria	Campos	Tabla llave Foránea	Campos
CLIENTS	CLI_IP	PGP_CLI	CLI_IP

4.5.2.11. Tabla VGP_CLI



Descripción: Esta tabla permite definirle a los grupos de VLANs los puertos de los switches a los que tendrán permiso.

Campo	Tipo	Longitud	Nulo
VGP_NAME	varchar	30	
CLI_IP	varchar	15	
CLI_PORTNAME	varchar	10	

Llaves primarias:

- VGP_NAME, CLI_IP, CLI_PORTNAME

Llaves foráneas:

- FK_VGP_CLI_VLAN_GROUPS

Tabla llave Primaria	Campos	Tabla llave Foránea	Campos
VLAN_GROUPS	VGP_NAME	VGP_CLI	VGP_NAME

- FK_VGP_CLI_CLIENTS

Tabla llave Primaria	Campos	Tabla llave Foránea	Campos
CLIENTS	CLI_IP	VGP_CLI	CLI_IP

4.5.2.12. Tabla VLN_PGP

Descripción: Esta tabla permite asociarle a las VLANs los Grupos de Puertos a los que tendrán acceso.

Campo	Tipo	Longitud	Nulo
VLN_NAME	varchar	30	
PGP_NAME	varchar	30	

Llaves primarias:

- VLN_NAME, PGP_NAME

Llaves foráneas:

- FK_VLN_PGP_VLANS

Tabla llave Primaria	Campos	Tabla llave Foránea	Campos
VLANS	VLN_NAME	VLN_PGP	VLN_NAME

- FK_VLN_PGP_PORT_GROUPS

Tabla llave Primaria	Campos	Tabla llave Foránea	Campos
PORT_GROUPS	PGP_NAME	VLN_PGP	PGP_NAME

4.5.2.13. Tabla VLN_VGP

Descripción: Esta tabla permite asociarle a los Grupos de VLANs las VLANs que los conformarán.

Campo	Tipo	Longitud	Nulo
VLN_NAME	varchar	30	
VGP_NAME	varchar	30	

Llaves primarias:

- VLN_NAME, VGP_NAME

Llaves foráneas:

- FK_VLN_VGP_VLANS

Tabla llave Primaria	Campos	Tabla llave Foránea	Campos
VLANS	VLN_NAME	VLN_VGP	VLN_NAME

- FK_VLN_VGP_VLAN_GROUPS

Tabla llave Primaria	Campos	Tabla llave Foránea	Campos
VLAN_GROUPS	VGP_NAME	VLN_VGP	VGP_NAME

4.5.2.14. Tabla VGP_PGP

Descripción: Esta tabla permite asociarle a los Grupos de VLANs los Grupos de Puertos a los que tendrán acceso.

Campo	Tipo	Longitud	Nulo
VGP_NAME	varchar	30	
PGP_NAME	varchar	30	

Llaves primarias:

- VGP_NAME, PGP_NAME

Llaves foráneas:

- FK_VGP_PGP_PORT_GROUPS

Tabla llave Primaria	Campos	Tabla llave Foránea	Campos
PORT_GROUPS	PGP_NAME	VGP_PGP	PGP_NAME

- FK_VGP_PGP_VLAN_GROUPS

Tabla llave Primaria	Campos	Tabla llave Foránea	Campos
VLAN_GROUPS	VGP_NAME	VGP_PGP	VGP_NAME

4.6. Puntos principales y comentarios

Este capítulo trató acerca del programa Free VMPS, en donde se describieron cada uno de sus componentes y la manera en que estos funcionan. A continuación, se exponen los puntos más importantes:

- El Free VMPS es un servidor VMPS, que se ha desarrollado para demostrar el uso de las VLANs dinámicas y documentar la estructura del protocolo VQP.

- Es un programa completamente gratis, que puede ayudar a centros educativos para que demuestren el uso de las VLANs dinámicas, y a las empresas, para que lo puedan implementar sin incurrir en gastos de software.

- El programa de configuración de la base de datos que se ha desarrollado, facilita la asignación de las membresías a las VLANs y ayuda a la solución de problemas.

- Con el Inspector de Redes, migrar de una red plana a una con VLANs dinámicas, es posible realizarlo en un plazo corto.

5. CONCLUSIONES

En base a la investigación realizada durante el desarrollo de este trabajo, se ha llegado a la conclusión que las VLANs son una herramienta eficaz para que los administradores de red puedan controlar patrones de tráfico (broadcasts), reaccionar a reubicaciones de equipo e incrementar el nivel de seguridad en la red. Aunque, la implementación de las VLANs puede llegar a ser una tarea complicada y tediosa, donde su mantenimiento puede requerir una excesiva cantidad de tiempo, se ha determinado que hay herramientas como el VMPS que pueden simplificar éstas tareas.

Con el VMPS, se pueden asignar VLANs dinámicamente y negar el acceso a los puertos de los switches utilizando la información almacenada en su archivo de configuración. Una limitante que posee, es la utilización del protocolo VQP que carece de mecanismos de seguridad, por lo tanto es necesario tomar precauciones en el momento de su implementación.

En el siguiente apartado, se enuncian algunas recomendaciones que se deben tomar en cuenta para una satisfactoria implementación del VMPS.

6. RECOMENDACIONES

- Se recomienda utilizar el modelo de VLANs local, porque son considerablemente más fáciles de administrar y conceptuar, están sujetas a menos limitantes en los equipos, y crean una menor dependencia del proveedor de servicio que las VLANs geográficas (VLANs de extremo a extremo).

- Con respecto a servidores, se recomienda ubicarlos lo más cerca posible del núcleo, teniendo un acceso rápido y equitativo a todos los puntos de la red. Esta recomendación se ve reforzada por la nueva regla 20/80, en donde se establece que el 20% del tráfico se mantiene localmente y el 80% se mueve fuera del grupo de trabajo.

- Al utilizar el VMPS, se necesita controlar los accesos a la VLAN administrativa. En el caso que el tráfico de la VLAN administrativa viaje fuera de la red, se deben utilizar técnicas de túneles y encripción, para evitar que los datagramas VQP interceptados y alterados.

- Se sugiere que el servidor en donde se instalará el Free VMPS, cumpla con los siguientes requisitos mínimos de hardware y software:
    - Procesador Pentimum 2 de 400 Mhz
    - 256 Mb en Ram
    - Disco duro de 10 Gb
    - Tarjeta de red
    - Sistema operativo Windows 2000
    - CD-Rom

- Con respecto a los switches, se recomienda utilizar modelos superiores a la serie Catalyst 1900, ya que estos carecen de ciertas funcionalidades, como la modificación del intervalo de reconfirmación.

- Evitar conectar hubs y switches a puertos configurados como dinámicos, ya que dependiendo del switch, se da de baja a la interfaz si se alcanza la cantidad máxima de hosts que pertenecen a la misma VLAN. La cantidad de host varía de plataforma.

7. APLICACIONES FUTURAS

El objetivo de este trabajo ha sido presentar el VMPS, como una herramienta para facilitar la administración de las redes. A partir de acá, pueden existir diferentes alternativas para implementar nuevas aplicaciones de esta herramienta.

Un ejemplo puede ser, el integrar un IDS con un VMPS para la mitigación de desastres por mal uso de la red local. Si se conecta un IDS a al puerto de monitoreo de un switch para la red local, y éste detecta que una PC está generando tráfico por la acción de un virus, podría mandar una alerta al VMPS. Luego, el VMPS se configuraría para que restrinja el acceso a ese host. A continuación, podría deshabilitar el puerto en donde se encuentra el host, por medio de una instrucción SNMP. El beneficio de ésta aplicación se encuentra en la prevención de futuras infecciones de otros equipos y la supresión de un tráfico malicioso.

Otra potencial aplicación del VMPS sería el manejar los ingresos a las VLANs dependiendo del usuario y la hora en que se realicen. Esto se puede aplicar en escenarios corporativos, campus universitarios, escuelas, hospitales y hoteles entre otros. Uniendo así, las capacidades del VMPS con protocolos AAA como el RADIUS, TACACS y KERBEROS, para autenticación, autorización y cobros por el servicio prestado.

Así como estos tipos de aplicaciones, es posible crear otras herramientas que automaticen el monitoreo y administración de los dispositivos de redes.

8. GLOSARIO

AAA: Autenticación Autorización Contabilización. Sistema de redes IP para identificar a que recursos informáticos tiene acceso el usuario y rastrear la actividad del usuario en la red. Autenticación es el proceso de identificación de un individuo, mediante un nombre de usuario y contraseña. Autorización es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que el usuario ha sido autenticado con éxito. Contabilización es el proceso de rastrear la actividad del usuario mientras accede a los recursos de la red. Los datos registrados se utilizan con fines estadísticos, facturación, auditoria y planeamiento de capacidad.

ADMINISTRADOR DE RED: Persona responsable de la operación, mantenimiento y administración de una red.

ACCESS POINT (Punto de Acceso): Es un receptor-transmisor de datos de redes inalámbricas, que utiliza ondas de radio para conectar una red cableada con dispositivos de red inalámbricos. Se podría comprender como un hub o switch que se comunica con dispositivos inalámbricos.

DES: Estándar de Encripción de Datos. Es un método estándar para la encripción y desencripción de datos, desarrollado por le buró Nacional de Estándares de los Estados Unidos. Trabaja por medio de la combinación de métodos de transposición y sustitución.

DIRECCIÓN IP: Dirección de 32 bits asignadas a *hosts* usando TCP/IP. Una dirección IP pertenece a una de las cinco clases (A, B, C, D ó E) y es escrita en 4 octetos separados por puntos. Cada dirección consiste de un número de red, a un número de subred opcional, y a un número de *host*. Los números de red y subred juntos son usados para enrutar, mientras que el número de *host* es usado para diferenciar a un *host* dentro de una red o subred. La máscara de red se usa para extraer la información de la red o subred de la dirección IP. También llamada dirección de Internet.

DIRECCIÓN MAC: Dirección estandarizada en la capa de enlace de datos que es requerida para cada puerto o dispositivo que se conecta a una *LAN*. Otros dispositivos en una red usan esta dirección para localizar puerto específicos en la red y para crear y actualizar tablas de enrutamiento y estructuras de datos. La dirección

MAC tiene 6 bytes de longitud y son controlados por la IEEE. También es conocida como dirección de hardware, dirección de capa-MAC, o dirección física.

DOMINIO DE DIFUSIÓN (Dominio de Broadcast): Es el conjunto de todos los dispositivos que recibirán tramas broadcast de cualquier dispositivo en el conjunto. Los dominios de broadcast están típicamente delimitados por routers porque no reenvían tramas de broadcast.

FULL DUPLEX: Es la capacidad de transmitir datos simultáneamente entre una estación origen y una destino.

HOST: Computadora en una red. Similar al término *nodo*, excepto que *host* usualmente implica una computadora y un *nodo* generalmente aplica a cualquier sistema en red, incluyendo servidores de acceso y routers.

HUB: Generalmente, un término usado para describir un dispositivo que sirve como centro de la topología de red en estrella. Dispositivo de Hardware o software que contiene múltiples módulos independientes de red y equipos de intranet. Los Hubs pueden ser activos (cuando repiten señales a través de ellos) o pasivos (cuando no repiten, pero solamente dividen señales enviadas a través de ellos). A veces es conocido como *concentrador*.

IDS: Sistema de detección de Intrusos. Es un software diseñado para detectar acciones específicas en una red que son específicas de un intruso o que puede indicar un acto de espionaje corporativo.

IEEE: Instituto de Ingenieros en Electricidad y Electrónica.

KERBEROS: Protocolo de autenticación de red que utiliza llaves secretas con el algoritmo criptográfico para encripción y autenticación DES.

LAN: Red de Área Local. Posee alta velocidad, pocos errores en los datos de la red, cubiertos en un área relativamente pequeña. Las LANs conectan estaciones de trabajo, periféricos, terminales, y otros dispositivos en un edificio o en otros en un área geográficamente limitada. Los estándares de una LAN especifican el cableado y señalización en las capas físicas y de enlace de datos del modelo OSI.

MAC (Media Access Control): Control de acceso al medio. Debajo de las dos sub-capas del enlace de datos definido por la IEEE. La sub-capa MAC, maneja los accesos a los medios compartidos.

NODO: Conexión final de una red o unión común de dos o más líneas en una red. Los nodos pueden ser procesadores, o estaciones de trabajo. Los nodos, los cuales varían en el enrutamiento y otras capacidades funcionales, pueden ser interconectados por enlaces, y sirven como puntos de control en una red. El término “nodo”, a veces es usado genéricamente para referirse a cualquier entidad que puede acceder a una red y es frecuentemente usado intercambiablemente con dispositivo.

PUERTO: 1) Interfaz en in dispositivo de intranet (como un router). 2) En la terminología IP, es un proceso de capa-superior que recibe información de las capas inferiores.

PROTOCOLO: Descripción formal de un conjunto de reglas y convenciones que gobiernan como los dispositivos de una red intercambian información.

RADIUS: Sistema cliente/servidor distribuido utilizado en AAA que permite evitar accesos a la red no autorizados.

RED: Colección de computadoras, impresoras, routers, switches y otros dispositivos que están habilitados para comunicarse con otros bajo algún medio de transmisión.

SNIFFER: Programa de para monitorear y analizar el tráfico en una red de computadoras, detectando los cuellos de botellas y problemas que existan en ella. Puede ser utilizado para "captar", lícitamente o no, los datos que son transmitidos en la red.

SSID (Service Set Identifier): Es también conocido como Nombre de Red de Radio. Es un identificador único, usado para identificar una red de radio y cuales dispositivos están permitidos comunicarse entre si o con un access point. El SSID puede consistir de hasta 32 caracteres alfanuméricos. Los SSIDs son sensibles a mayúsculas y minúsculas.

SWITCH: 1) Dispositivo de red que filtra, reenvía e inunda de tramas basado en la dirección de destino de cada trama. 2) Término general aplicado a un dispositivo electrónico o mecánico que permite que sea establecida una conexión cuando sea necesario y terminada cuando ya no exista una sesión que la soporte.

SWITCH DE LAN: Switch de alta velocidad que reenvía paquetes entre segmentos de la capa de enlace. Muchos switches de LAN reenvían el tráfico basados en la *dirección MAC*. Esta variedad de switches de LAN son a veces llamados *switches de*

tramas. Los switches de LAN a menudo son categorizados de acuerdo al método que utilizan para reenviar el tráfico: método de corte o método de almacenamiento y envío. Los switches multicapa son un conjunto inteligente de switches de LAN.

TACACS: Sistema de Control de Acceso para el Controlador de Acceso a la Terminal. Protocolo de autenticación que provee de autenticación de acceso remoto y servicios relacionados, como bitácora de eventos. Las contraseñas de los usuarios son administradas en una base de datos centralizada, en lugar de routers individuales, suministrando una solución fácilmente escalable para la seguridad de la red.

UDP (User Datagram Protocol): Protocolo de Datagramas de Usuario. Protocolo de capa de transporte no orientado a conexión en la pila del protocolos TCP/IP. UDP es un protocolo simple que intercambia datagramas sin acuses de recibos o sin que se garantice su recepción, requiriendo que el procesamiento de los errores y retransmisión sea manejado por otros protocolos. UDP está definido en la RFC 768.

VLAN (Virtual LAN): Grupo de dispositivos en una LAN que están configurados (usando un software de administración) para que se puedan comunicar como si estuvieran conectados en el mismo cable, cuando en la realidad se encuentran localizados en un número diferentes de segmentos de LAN. Porque las VLANs están basadas en conexiones lógicas en vez de físicas, son extremadamente flexibles.

WEP (Wired Equivalent Privacy): es un estándar 802.11 opcional de encriptación de datos para su transmisión en redes inalámbricas (redes de radio). Es implementado en la capa de red (capa 2 del modelo OSI) en la mayoría de tarjetas de redes inalámbricas y access point que actualmente se venden.

9. BIBLIOGRAFÍA

- A. Anthony Bruno, Jacqueline Kim [2000], CCDA Exam Certification Guide, Cisco Press, Indianapolis, USA.

- Odom, Wendell [2004], CCNA ICND Exam Certification Guide, Cisco Press, Indianapolis, USA.

- Lammle, Todd [2004], CCNA Cisco Certified Network Associate Study Guide, SYBEX, Inc., California, USA.

- Spurgeon, Charles E. [2000], Ethernet The Definitive Guide, O'Relly, California, USA.

- Feibel, Werner [1996], The Encyclopedia of Networking, SYBEX, Inc. California, USA.

- James G. Jones, Sheldon Barry [2003], CCNA Exam Cram 2, Que Publishing, USA.

- Odom, Sean [2003], CCNP CIT Exam Cram 2, Que Publishing, USA.

- Jeffrey L. Whitten, Lonnie D. Bentley, Victor M. Barlow [2000], Análisis y Diseño de Sistemas de Información, 3a Edición, Editorial Nomos S. A., Colombia.

- Marco Cantú [2003], Mastering Delphi 7, Sybex.

- Ray Lischner [2000], Delphi in a Nutshell, O'Reilly & Associates Inc., USA.

- Kurt Bittner, Ian Spence [2002], Use Case Modeling, Addison Wesley.

- Peter Dyson [1995], Dictionary of Networking, Sybex.

9.1 Páginas Web

- Olenchek, Jeff, Jeff Olenchek's VMPS Page, http://www.uwm.edu/~jeff/doc/vmps/index.html

- The COEIT Client Validation Program, http://www.engr.sc.edu

- Data Flow Diagrams, http://www.cems.uwe.ac.uk/~tdrewry/dfds.htm

- Incorporating Wireless Devices into VLANs, http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1100/accsspts/i12213ja/i12213sc/s13vlan.htm

- Conceptos y Vulneabilidades del WEP, http://www.wi-fiplanet.com/tutorials/article.php/1368661

10. ANEXOS

10.1 Pruebas de tramas VQP

Prueba No. 1

Objetivo:	
Obtener la trama que envía un cliente, en donde le pida al VMPS el ingreso a la red de un host.	
Configuración inicial VMPS y Switch:	
Modo: no seguro Default VLAN: --NONE— No-domain-req: deny	Dominio: KRYPTOS VLANs: PRUEBA
Trama de Consulta:	

```
                                  01 01 00 06 0a 00              ......
00 00 00 00 0c 01 00 04 c0 a8 03 96 00 00 0c 02   ................
00 02 31 35 00 00 0c 03 00 08 2d 2d 4e 4f 4e 45   ..15......--NONE
2d 2d 00 00 0c 04 00 07 4b 52 59 50 54 4f 53 00   --......KRYPTOS.
00 0c 07 00 01 00 00 00 0c 06 00 06 00 02 2d 1a   ..............-.
a0 9e
..
```

Trama de Respuesta:
Conclusión:

Prueba No. 2

Objetivo:

Obtener la trama de respuesta del VMPS, cuando el cliente le solicita el ingreso de un host a la red.

Configuración inicial VMPS y Switch:

Modo: no seguro Default VLAN: --NONE— No-domain-req: deny	Dominio: KRYPTOS VLANs: PRUEBA

Trama de Consulta:

```
                                  01 01 00 06 15 00              ......
00 00 00 00 0c 01 00 04 c0 a8 03 96 00 00 0c 02   ................
00 02 31 30 00 00 0c 03 00 08 2d 2d 4e 4f 4e 45   ..10......--NONE
2d 2d 00 00 0c 04 00 07 4b 52 59 50 54 4f 53 00   --......KRYPTOS.
00 0c 07 00 01 00 00 00 0c 06 00 06 00 02 2d 1a   ..............-.
a0 9e                                             ..
```

Trama de Respuesta:

```
                                  01 02 00 02 15 00              ......
00 00 00 00 0c 03 00 06 50 52 55 45 42 41 00 00   ........PRUEBA..
0c 08 00 06 00 02 2d 1a a0 9e                     ......-...
```

Conclusión:

Prueba No. 3

Objetivo:

Obtener la trama de negación de conexión de un cliente, trabajando el vmps en modo no seguro.

Configuración inicial VMPS y Switch:

Modo: no seguro Default VLAN: --NONE— No-domain-req: deny	Dominio: KRYPTOS VLANs: PRUEBA

Trama de Consulta:

```
                                  01 01 00 06 16 00                ......
00 00 00 00 0c 01 00 04 c0 a8 03 96 00 00 0c 02   ................
00 02 31 34 00 00 0c 03 00 08 2d 2d 4e 4f 4e 45   ..14......--NONE
2d 2d 00 00 0c 04 00 07 4b 52 59 50 54 4f 53 00   --......KRYPTOS.
00 0c 07 00 01 00 00 00 0c 06 00 06 00 02 2d 1a   ..............-.
a0 9e                                             ..
```

Trama de Respuesta:

```
                                  01 02 03 00 16 00                ......
00 00                                             ..
```

Conclusión:

Prueba No. 4

Objetivo:

Obtener la trama de negación de conexión de un cliente, trabajando el vmps en modo seguro.

Configuración inicial VMPS y Switch:

Modo: seguro Default VLAN: --NONE— No-domain-req: deny	Dominio: KRYPTOS VLANs: PRUEBA

Trama de Consulta:

```
                                01 01 00 06 20 00              ......
00 00 00 00 0c 01 00 04 c0 a8 03 96 00 00 0c 02   ................
00 02 31 34 00 00 0c 03 00 08 2d 2d 4e 4f 4e 45   ..14......--NONE
2d 2d 00 00 0c 04 00 07 4b 52 59 50 54 4f 53 00   --......KRYPTOS.
00 0c 07 00 01 00 00 00 0c 06 00 06 00 02 2d 1a   ..............-.
a0 9e                                             ..
```

Trama de Respuesta:

```
                                01 02 04 00 20 00              ......
00 00                                             ..
```

Conclusión:

Prueba No. 5

Objetivo:

Obtener la trama de error de versión de protocolo

Configuración inicial VMPS y Switch:

Modo: seguro Default VLAN: --NONE— No-domain-req: deny	Dominio: KRYPTOS VLANs: PRUEBA

Trama de Consulta:

```
                                01 01 00 06 07 00              ......
00 00 00 00 0c 01 00 04 c0 a8 03 c8 00 00 0c 02   ................
00 02 31 34 00 00 0c 03 00 08 2d 2d 4e 4f 4e 45   ..14......--NONE
2d 2d 00 00 0c 04 00 07 4b 52 59 50 54 4f 53 00   --......KRYPTOS.
00 0c 07 00 01 00 00 00 0c 06 00 06 00 d0 09 70   ...............p
84 9e                                             ..
```

Trama de Respuesta:

```
                                01 02 01 00 07 00   ...5....^.......
00 00                                               ..............
```

Conclusión:

El switch marca que esta el la trama correcta

Prueba No. 6

Objetivo:

Obtener la trama de no hay recursos

Configuración inicial VMPS y Switch:

Modo: seguro Default VLAN: --NONE— No-domain-req: deny	Dominio: KRYPTOS VLANs: PRUEBA

Trama de Consulta:

```
                                  01 01 00 06 08 00              ......
00 00 00 00 0c 01 00 04 c0 a8 03 c8 00 00 0c 02   ................
00 02 31 34 00 00 0c 03 00 08 2d 2d 4e 4f 4e 45   ..14......--NONE
2d 2d 00 00 0c 04 00 07 4b 52 59 50 54 4f 53 00   --......KRYPTOS.
00 0c 07 00 01 00 00 00 0c 06 00 06 00 d0 09 70   ...............p
84 9e                                             ..
```

Trama de Respuesta:

```
                                  01 02 02 00 07 00   ...5....^.......
00 00                                                 ..............
```

Conclusión:

El switch marca que esta la trama es correcta

Prueba No. 7

Objetivo:

Obtener la trama que envía un cliente, en donde le pida al VMPS el ingreso a la red de un host, sin configurar el dominio en el switch.

Configuración inicial VMPS y Switch:

Modo: no seguro Default VLAN: --NONE— No-domain-req: deny	Dominio: VLANs: PRUEBA

Trama de Consulta:

```
                                 01 01 00 05 01 00   .}...5.CP6......
00 00 00 00 0c 01 00 04 c0 a8 03 c8 00 00 0c 02   ................
00 02 31 30 00 00 0c 03 00 08 2d 2d 4e 4f 4e 45   ..10......--NONE
2d 2d 00 00 0c 07 00 01 00 00 00 0c 06 00 06 00   --..............
04 ac 9d fc 4b                                    ....K
```

Trama de Respuesta:

Conclusión:

El cuarto bit cambió a 05 y en los datos no viene `00 00 0c 04`

10.2 Guión de Instalación de la Base de Datos en MySQL

```
#mysql> connect vmp
connect vmps

##################################
#                                #
#    Borrado de las tablas       #
#                                #
##################################


DROP TABLE VLN_VGP;
DROP TABLE VLN_PGP;
DROP TABLE VLN_CLI;
DROP TABLE VGP_PGP;
DROP TABLE VGP_CLI;
DROP TABLE PGP_CLI;
DROP TABLE VLAN_GROUPS;
DROP TABLE PORT_GROUPS;
DROP TABLE HOSTS;
DROP TABLE VLANS;
DROP TABLE CLIENTS;
DROP TABLE APP_USERMENU;
DROP TABLE APP_MENU;
DROP TABLE APP_USERS;

##################################
#                                #
#      Eliminación de base de datos      #
#                                #
##################################
```

```
DROP DATABASE VMPS;


##################################
#                                #
#     Creación de la base de datos     #
#                                #
##################################

CREATE DATABASE VMPS;
USE VMPS;


##################################
#                                #
#          Creación de las tablas          #
#                                #
##################################

#
# Creación de la tabla APP_MENU
#

CREATE TABLE APP_MENU (
  MNU_IDMENU int(11) NOT NULL auto_increment,
  MNU_NAME varchar(50) NOT NULL default '',
  MNU_TIPO int(11) NOT NULL default '0',
  MNU_URL varchar(50) NOT NULL default 'construc.php',
  PRIMARY KEY (MNU_IDMENU)
) TYPE=InnoDB AUTO_INCREMENT=3;
```

```
#
# Creación de la tabla APP_USERS
#

CREATE TABLE APP_USERS (
  USR_NAME varchar(30) NOT NULL default '',
  USR_USERNAME varchar(30) NOT NULL default '',
  USR_PASSWORD varchar(40) NOT NULL default '',
  USR_EMAIL varchar(50) default NULL,
  PRIMARY KEY (USR_USERNAME)
) TYPE=InnoDB;



#
# Creación de la tabla APP_USERMENU
#

CREATE TABLE APP_USERMENU (
  USM_USERNAME varchar(30) NOT NULL default '0',
  USM_IDMENU int(11) NOT NULL default '0',
  PRIMARY KEY PK_USERMENU (USM_USERNAME,USM_IDMENU),
  FOREIGN KEY (USM_USERNAME) REFERENCES APP_USERS
(USR_USERNAME),
        INDEX (USM_IDMENU),
        FOREIGN KEY (USM_IDMENU) REFERENCES APP_MENU
(MNU_IDMENU)
) TYPE=InnoDB;

#
# Creación de la tabla CLIENTS
#
```

```
CREATE TABLE CLIENTS (
  CLI_IP varchar(15) NOT NULL default '',
  CLI_NAME varchar(150) NOT NULL default '',
  CLI_DESCRIPTION varchar(50) NULL default '',
  CLI_PORTS int(11) NULL default '0',
  CLI_BRAND varchar(25) NULL default '',
  CLI_MODEL varchar(25) NULL default '',
  CLI_SERIE varchar(25) NULL default '',
  CLI_SNMPRO varchar(15) NOT NULL default 'public',
  CLI_SNMPWR varchar(15) NOT NULL default 'private',
  PRIMARY KEY (CLI_IP)
) TYPE=InnoDB;


#
# Creación de la tabla VLANS
#

CREATE TABLE VLANS (
        VLN_NAME varchar(30) NOT NULL default '',
        VLN_DESCRIPTION varchar(50) NULL default '',
        PRIMARY KEY (VLN_NAME)
) TYPE=InnoDB;


#
# Creación de la tabla HOSTS
#

CREATE TABLE HOSTS (
        HST_MAC varchar(17) NOT NULL default '',
        HST_NAME varchar(50) NOT NULL default '',
```

```
        VLN_NAME varchar(30) NOT NULL default '',
        HST_DESCRIPTION varchar(50) NULL default '',
        HST_IP varchar(15) NULL default '',
        HST_INSERT_DATE datetime NOT NULL default '',
        PRIMARY KEY (HST_MAC),
        INDEX (VLN_NAME),
        FOREIGN KEY (VLN_NAME) REFERENCES VLANS (VLN_NAME)
) TYPE=InnoDB;


#
# Creación de la tabla PORT_GROUPS
#

CREATE TABLE PORT_GROUPS (
        PGP_NAME varchar(30) NOT NULL default '',
        PGP_DESCRIPTION varchar(50) NOT NULL default '',
        PRIMARY KEY (PGP_NAME)
) TYPE=InnoDB;


#
# Creación de la tabla VLAN_GROUPS
#

CREATE TABLE VLAN_GROUPS (
        VGP_NAME varchar(30) NOT NULL default '',
        VGP_DESCRIPTION varchar(50) NULL default '',
        PRIMARY KEY (VGP_NAME)
) TYPE=InnoDB;
```

```
#
# Creación de la tabla PGP_CLI
#

CREATE TABLE PGP_CLI (
        PGP_NAME varchar(30) NOT NULL default '',
        CLI_IP varchar(15) NOT NULL default '',
        CLI_PORTNAME varchar(10) NOT NULL,
        KEY PK_PGP_CLI (PGP_NAME,CLI_IP,CLI_PORTNAME),
        FOREIGN KEY (PGP_NAME) REFERENCES PORT_GROUPS
(PGP_NAME),
        INDEX (CLI_IP),
        FOREIGN KEY (CLI_IP) REFERENCES CLIENTS (CLI_IP)
) TYPE=InnoDB;



#
# Creación de la tabla VGP_CLI
#

CREATE TABLE VGP_CLI (
        VGP_NAME varchar(30) NOT NULL default '',
        CLI_IP varchar(15) NOT NULL default '',
        CLI_PORTNAME varchar(10) NOT NULL,
        PRIMARY KEY PK_VGP_CLI (VGP_NAME,CLI_IP,CLI_PORTNAME),
        FOREIGN KEY (VGP_NAME) REFERENCES VLAN_GROUPS
(VGP_NAME),
        INDEX (CLI_IP),
        FOREIGN KEY (CLI_IP) REFERENCES CLIENTS (CLI_IP)
) TYPE=InnoDB;
```

```
#
# Creación de la tabla VGP_PGP
#

CREATE TABLE VGP_PGP (
        VGP_NAME varchar(30) NOT NULL default '',
        PGP_NAME varchar(30) NOT NULL default '',
        PRIMARY KEY PK_VLN_VGP (VGP_NAME,PGP_NAME),
        FOREIGN KEY (VGP_NAME) REFERENCES VLAN_GROUPS
(VGP_NAME),
        INDEX (PGP_NAME),
        FOREIGN KEY (PGP_NAME) REFERENCES PORT_GROUPS (PGP_NAME)

) TYPE=InnoDB;

#
# Creación de la tabla VLN_CLI
#

CREATE TABLE VLN_CLI (
        VLN_NAME varchar(30) NOT NULL default '',
        CLI_IP varchar(15) NOT NULL default '',
        CLI_PORTNAME varchar(10) NOT NULL,
        PRIMARY KEY PK_VLN_CLI (VLN_NAME,CLI_IP,CLI_PORTNAME),
        FOREIGN KEY (VLN_NAME) REFERENCES VLANS (VLN_NAME),
        INDEX (CLI_IP),
        FOREIGN KEY (CLI_IP) REFERENCES CLIENTS (CLI_IP)
) TYPE=InnoDB;



#
```

```
# Creación de la tabla VLN_PGP
#

CREATE TABLE VLN_PGP (
        VLN_NAME varchar(30) NOT NULL default '',
        PGP_NAME varchar(30) NOT NULL default '',
        PRIMARY KEY PK_VLN_PGP (VLN_NAME,PGP_NAME),
        FOREIGN KEY (VLN_NAME) REFERENCES VLANS (VLN_NAME),
        INDEX (pGP_NAME),
        FOREIGN KEY (PGP_NAME) REFERENCES PORT_GROUPS (PGP_NAME)
) TYPE=InnoDB;



#
# Creación de la tabla VLN_VGP
#

CREATE TABLE VLN_VGP (
        VLN_NAME varchar(30) NOT NULL default '',
        VGP_NAME varchar(30) NOT NULL default '',
        PRIMARY KEY PK_VLN_VGP (VLN_NAME,VGP_NAME),
        FOREIGN KEY (VLN_NAME) REFERENCES VLANS (VLN_NAME),
        INDEX (VGP_NAME),
        FOREIGN KEY (VGP_NAME) REFERENCES VLAN_GROUPS (VGP_NAME)
) TYPE=InnoDB;

##################################
#                                #
#          Llenado de las tablas #
#                                #
##################################
```

```
#
# Llenado de la tabla APP_MENU
#

INSERT INTO APP_MENU (MNU_IDMENU, MNU_NAME, MNU_TIPO, MNU_URL)
VALUES (1, 'Administración de Usuarios del Sistema', 1, 'adminusers.php');
INSERT INTO APP_MENU (MNU_IDMENU, MNU_NAME, MNU_TIPO, MNU_URL)
VALUES (2, 'Administración del Servidor VMPS', 0, 'admserver.php');
INSERT INTO VLANS (VLN_NAME, VLN_DESCRIPTION) VALUES (
'--NONE--', '');
INSERT INTO APP_USERS (USR_NAME, USR_USERNAME, USR_PASSWORD,
USR_EMAIL) VALUES ( 'Administrador VMPS', 'adminvmps',
‘eaf560cec71653ea1ee33e76acb467f8’, 'adminvmps@company.com');
INSERT INTO APP_USERMENU (USM_USERNAME, USM_IDMENU) VALUES (
'adminvmps', '1');
INSERT INTO APP_USERMENU (USM_USERNAME, USM_IDMENU) VALUES (
'adminvmps', '2');
```

10.3 Guión de Instalación de la Base de Datos en Microsoft SQL Server

```
if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[FK_APP_USERMENU_APP_MENU]') and
OBJECTPROPERTY(id, N'IsForeignKey') = 1)
ALTER TABLE [dbo].[APP_USERMENU] DROP CONSTRAINT
FK_APP_USERMENU_APP_MENU
GO

if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[FK_APP_USERMENU_APP_USERS]') and
OBJECTPROPERTY(id, N'IsForeignKey') = 1)
ALTER TABLE [dbo].[APP_USERMENU] DROP CONSTRAINT
FK_APP_USERMENU_APP_USERS
GO
```

```
if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[FK_PGP_CLI_CLIENTS]') and OBJECTPROPERTY(id,
N'IsForeignKey') = 1)
ALTER TABLE [dbo].[PGP_CLI] DROP CONSTRAINT FK_PGP_CLI_CLIENTS
GO

if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[FK_VGP_CLI_CLIENTS]') and OBJECTPROPERTY(id,
N'IsForeignKey') = 1)
ALTER TABLE [dbo].[VGP_CLI] DROP CONSTRAINT FK_VGP_CLI_CLIENTS
GO

if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[FK_VLN_CLI_CLIENTS]') and OBJECTPROPERTY(id,
N'IsForeignKey') = 1)
ALTER TABLE [dbo].[VLN_CLI] DROP CONSTRAINT FK_VLN_CLI_CLIENTS
GO

if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[FK_PGP_CLI_PORT_GROUPS]') and OBJECTPROPERTY(id,
N'IsForeignKey') = 1)
ALTER TABLE [dbo].[PGP_CLI] DROP CONSTRAINT
FK_PGP_CLI_PORT_GROUPS
GO

if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[FK_VGP_PGP_PORT_GROUPS]') and OBJECTPROPERTY(id,
N'IsForeignKey') = 1)
ALTER TABLE [dbo].[VGP_PGP] DROP CONSTRAINT
FK_VGP_PGP_PORT_GROUPS
GO
```

```
if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[FK_VLN_PGP_PORT_GROUPS]') and OBJECTPROPERTY(id,
N'IsForeignKey') = 1)
ALTER TABLE [dbo].[VLN_PGP] DROP CONSTRAINT
FK_VLN_PGP_PORT_GROUPS
GO

if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[FK_HOSTS_VLANS]') and OBJECTPROPERTY(id,
N'IsForeignKey') = 1)
ALTER TABLE [dbo].[HOSTS] DROP CONSTRAINT FK_HOSTS_VLANS
GO

if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[FK_VLN_CLI_VLANS]') and OBJECTPROPERTY(id,
N'IsForeignKey') = 1)
ALTER TABLE [dbo].[VLN_CLI] DROP CONSTRAINT FK_VLN_CLI_VLANS
GO

if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[FK_VLN_PGP_VLANS]') and OBJECTPROPERTY(id,
N'IsForeignKey') = 1)
ALTER TABLE [dbo].[VLN_PGP] DROP CONSTRAINT FK_VLN_PGP_VLANS
GO

if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[FK_VLN_VGP_VLANS]') and OBJECTPROPERTY(id,
N'IsForeignKey') = 1)
ALTER TABLE [dbo].[VLN_VGP] DROP CONSTRAINT FK_VLN_VGP_VLANS
GO
```

```
if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[FK_VGP_CLI_VLAN_GROUPS]') and OBJECTPROPERTY(id,
N'IsForeignKey') = 1)
ALTER TABLE [dbo].[VGP_CLI] DROP CONSTRAINT
FK_VGP_CLI_VLAN_GROUPS
GO

if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[FK_VGP_PGP_VLAN_GROUPS]') and OBJECTPROPERTY(id,
N'IsForeignKey') = 1)
ALTER TABLE [dbo].[VGP_PGP] DROP CONSTRAINT
FK_VGP_PGP_VLAN_GROUPS
GO

if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[FK_VLN_VGP_VLAN_GROUPS]') and OBJECTPROPERTY(id,
N'IsForeignKey') = 1)
ALTER TABLE [dbo].[VLN_VGP] DROP CONSTRAINT
FK_VLN_VGP_VLAN_GROUPS
GO

if exists (select * from dbo.sysobjects where id = object_id(N'[dbo].[APP_MENU]') and
OBJECTPROPERTY(id, N'IsUserTable') = 1)
drop table [dbo].[APP_MENU]
GO

if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[APP_USERMENU]') and OBJECTPROPERTY(id, N'IsUserTable')
= 1)
drop table [dbo].[APP_USERMENU]
GO
```

```
if exists (select * from dbo.sysobjects where id = object_id(N'[dbo].[APP_USERS]')
and OBJECTPROPERTY(id, N'IsUserTable') = 1)
drop table [dbo].[APP_USERS]
GO

if exists (select * from dbo.sysobjects where id = object_id(N'[dbo].[CLIENTS]') and
OBJECTPROPERTY(id, N'IsUserTable') = 1)
drop table [dbo].[CLIENTS]
GO

if exists (select * from dbo.sysobjects where id = object_id(N'[dbo].[HOSTS]') and
OBJECTPROPERTY(id, N'IsUserTable') = 1)
drop table [dbo].[HOSTS]
GO

if exists (select * from dbo.sysobjects where id = object_id(N'[dbo].[PGP_CLI]') and
OBJECTPROPERTY(id, N'IsUserTable') = 1)
drop table [dbo].[PGP_CLI]
GO

if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[PORT_GROUPS]') and OBJECTPROPERTY(id, N'IsUserTable') =
1)
drop table [dbo].[PORT_GROUPS]
GO

if exists (select * from dbo.sysobjects where id = object_id(N'[dbo].[VGP_CLI]') and
OBJECTPROPERTY(id, N'IsUserTable') = 1)
drop table [dbo].[VGP_CLI]
GO
```

```
if exists (select * from dbo.sysobjects where id = object_id(N'[dbo].[VGP_PGP]') and
OBJECTPROPERTY(id, N'IsUserTable') = 1)
drop table [dbo].[VGP_PGP]
GO

if exists (select * from dbo.sysobjects where id = object_id(N'[dbo].[VLANS]') and
OBJECTPROPERTY(id, N'IsUserTable') = 1)
drop table [dbo].[VLANS]
GO

if exists (select * from dbo.sysobjects where id = object_id(N'[dbo].[VLAN_GROUPS]')
and OBJECTPROPERTY(id, N'IsUserTable') = 1)
drop table [dbo].[VLAN_GROUPS]
GO

if exists (select * from dbo.sysobjects where id = object_id(N'[dbo].[VLN_CLI]') and
OBJECTPROPERTY(id, N'IsUserTable') = 1)
drop table [dbo].[VLN_CLI]
GO

if exists (select * from dbo.sysobjects where id = object_id(N'[dbo].[VLN_PGP]') and
OBJECTPROPERTY(id, N'IsUserTable') = 1)
drop table [dbo].[VLN_PGP]
GO

if exists (select * from dbo.sysobjects where id = object_id(N'[dbo].[VLN_VGP]') and
OBJECTPROPERTY(id, N'IsUserTable') = 1)
drop table [dbo].[VLN_VGP]
GO

CREATE TABLE [dbo].[APP_MENU] (
        [MNU_IDMENU] [int] NOT NULL ,
```

```
	[MNU_NAME] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NOT NULL ,
	[MNU_TIPO] [int] NOT NULL ,
	[MNU_URL] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS NOT
NULL
) ON [PRIMARY]
GO

CREATE TABLE [dbo].[APP_USERMENU] (
	[USM_USERNAME] [varchar] (30) COLLATE
SQL_Latin1_General_CP1_CI_AS NOT NULL ,
	[USM_IDMENU] [int] NOT NULL
) ON [PRIMARY]
GO

CREATE TABLE [dbo].[APP_USERS] (
	[USR_USERNAME] [varchar] (30) COLLATE
SQL_Latin1_General_CP1_CI_AS NOT NULL ,
	[USR_NAME] [varchar] (30) COLLATE SQL_Latin1_General_CP1_CI_AS
NOT NULL ,
	[USR_PASSWORD] [varchar] (40) COLLATE
SQL_Latin1_General_CP1_CI_AS NOT NULL ,
	[USR_EMAIL] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NULL
) ON [PRIMARY]
GO

CREATE TABLE [dbo].[CLIENTS] (
	[CLI_IP] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS NOT
NULL ,
	[CLI_NAME] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS NOT
NULL ,
```

```
	[CLI_DESCRIPTION] [varchar] (50) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
	[CLI_PORTS] [int] NULL ,
	[CLI_BRAND] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NULL ,
	[CLI_MODEL] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NULL ,
	[CLI_SERIE] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NULL ,
	[CLI_SNMPRO] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NOT NULL ,
	[CLI_SNMPWR] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NOT NULL
) ON [PRIMARY]
GO

CREATE TABLE [dbo].[HOSTS] (
	[HST_MAC] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS NOT
NULL ,
	[HST_NAME] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NOT NULL ,
	[VLN_NAME] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NOT NULL ,
	[HST_DESCRIPTION] [varchar] (50) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
	[HST_IP] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
	[HST_INSERT_DATE] [datetime] NOT NULL
) ON [PRIMARY]
GO

CREATE TABLE [dbo].[PGP_CLI] (
```

```
	[PGP_NAME] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NOT NULL ,
	[CLI_IP] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS NOT
NULL ,
	[CLI_PORTNAME] [varchar] (50) COLLATE
SQL_Latin1_General_CP1_CI_AS NOT NULL
) ON [PRIMARY]
GO

CREATE TABLE [dbo].[PORT_GROUPS] (
	[PGP_NAME] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NOT NULL ,
	[PGP_DESCRIPTION] [varchar] (50) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL
) ON [PRIMARY]
GO

CREATE TABLE [dbo].[VGP_CLI] (
	[VGP_NAME] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NOT NULL ,
	[CLI_IP] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS NOT
NULL ,
	[CLI_PORTNAME] [varchar] (50) COLLATE
SQL_Latin1_General_CP1_CI_AS NOT NULL
) ON [PRIMARY]
GO

CREATE TABLE [dbo].[VGP_PGP] (
	[VGP_NAME] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NOT NULL ,
	[PGP_NAME] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NOT NULL
```

```
) ON [PRIMARY]
GO

CREATE TABLE [dbo].[VLANS] (
	[VLN_NAME] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NOT NULL ,
	[VLN_DESCRIPTION] [varchar] (50) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL
) ON [PRIMARY]
GO

CREATE TABLE [dbo].[VLAN_GROUPS] (
	[VGP_NAME] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NOT NULL ,
	[VGP_DESCRIPTION] [varchar] (50) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL
) ON [PRIMARY]
GO

CREATE TABLE [dbo].[VLN_CLI] (
	[VLN_NAME] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NOT NULL ,
	[CLI_IP] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS NOT
NULL ,
	[CLI_PORTNAME] [varchar] (50) COLLATE
SQL_Latin1_General_CP1_CI_AS NOT NULL
) ON [PRIMARY]
GO

CREATE TABLE [dbo].[VLN_PGP] (
	[VLN_NAME] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NOT NULL ,
```

```
	[PGP_NAME] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NOT NULL
) ON [PRIMARY]
GO

CREATE TABLE [dbo].[VLN_VGP] (
	[VLN_NAME] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NOT NULL ,
	[VGP_NAME] [varchar] (50) COLLATE SQL_Latin1_General_CP1_CI_AS
NOT NULL
) ON [PRIMARY]
GO

ALTER TABLE [dbo].[APP_MENU] WITH NOCHECK ADD
	CONSTRAINT [PK_Menus] PRIMARY KEY  CLUSTERED
	(
		[MNU_IDMENU]
	)  ON [PRIMARY]
GO

ALTER TABLE [dbo].[APP_USERMENU] WITH NOCHECK ADD
	CONSTRAINT [PK_USERMENU] PRIMARY KEY  CLUSTERED
	(
		[USM_USERNAME],
		[USM_IDMENU]
	)  ON [PRIMARY]
GO

ALTER TABLE [dbo].[APP_USERS] WITH NOCHECK ADD
	CONSTRAINT [PK_USUARIOS] PRIMARY KEY  CLUSTERED
	(
		[USR_USERNAME]
```

```
	)  ON [PRIMARY]
GO

ALTER TABLE [dbo].[CLIENTS] WITH NOCHECK ADD
	CONSTRAINT [PK_CLIENTS] PRIMARY KEY  CLUSTERED
	(
		[CLI_IP]
	)  ON [PRIMARY]
GO

ALTER TABLE [dbo].[HOSTS] WITH NOCHECK ADD
	CONSTRAINT [PK_HOSTS] PRIMARY KEY  CLUSTERED
	(
		[HST_MAC]
	)  ON [PRIMARY]
GO

ALTER TABLE [dbo].[PGP_CLI] WITH NOCHECK ADD
	CONSTRAINT [PK_PGP_CLI] PRIMARY KEY  CLUSTERED
	(
		[PGP_NAME],
		[CLI_IP],
		[CLI_PORTNAME]
	)  ON [PRIMARY]
GO

ALTER TABLE [dbo].[PORT_GROUPS] WITH NOCHECK ADD
	CONSTRAINT [PK_PORT_GROUPS] PRIMARY KEY  CLUSTERED
	(
		[PGP_NAME]
	)  ON [PRIMARY]
GO
```

```
ALTER TABLE [dbo].[VGP_CLI] WITH NOCHECK ADD
	CONSTRAINT [PK_VGP_CLI] PRIMARY KEY  CLUSTERED
	(
		[VGP_NAME],
		[CLI_IP],
		[CLI_PORTNAME]
	)  ON [PRIMARY]
GO

ALTER TABLE [dbo].[VGP_PGP] WITH NOCHECK ADD
	CONSTRAINT [PK_VGP_PGP] PRIMARY KEY  CLUSTERED
	(
		[VGP_NAME],
		[PGP_NAME]
	)  ON [PRIMARY]
GO

ALTER TABLE [dbo].[VLANS] WITH NOCHECK ADD
	CONSTRAINT [PK_VLANS] PRIMARY KEY  CLUSTERED
	(
		[VLN_NAME]
	)  ON [PRIMARY]
GO

ALTER TABLE [dbo].[VLAN_GROUPS] WITH NOCHECK ADD
	CONSTRAINT [PK_VLAN_GROUP] PRIMARY KEY  CLUSTERED
	(
		[VGP_NAME]
	)  ON [PRIMARY]
GO
```

```
ALTER TABLE [dbo].[VLN_CLI] WITH NOCHECK ADD
	CONSTRAINT [PK_VLN_CLI] PRIMARY KEY  CLUSTERED
	(
		[VLN_NAME],
		[CLI_IP],
		[CLI_PORTNAME]
	)  ON [PRIMARY]
GO

ALTER TABLE [dbo].[VLN_PGP] WITH NOCHECK ADD
	CONSTRAINT [PK_VLN_PGP] PRIMARY KEY  CLUSTERED
	(
		[VLN_NAME],
		[PGP_NAME]
	)  ON [PRIMARY]
GO

ALTER TABLE [dbo].[VLN_VGP] WITH NOCHECK ADD
	CONSTRAINT [PK_VLN_VGP] PRIMARY KEY  CLUSTERED
	(
		[VLN_NAME],
		[VGP_NAME]
	)  ON [PRIMARY]
GO

ALTER TABLE [dbo].[APP_MENU] ADD
	CONSTRAINT [DF_MENUS_MNU_IDMENU] DEFAULT (0) FOR
[MNU_IDMENU],
	CONSTRAINT [DF_MENUS_MNU_TIPO] DEFAULT (0) FOR [MNU_TIPO],
	CONSTRAINT [DF_MENUS_MNU_URL] DEFAULT ('construc.php') FOR
[MNU_URL]
GO
```

```
ALTER TABLE [dbo].[APP_USERMENU] ADD
	CONSTRAINT [DF_USERMENU_IDUsuario] DEFAULT (0) FOR
[USM_USERNAME],
	CONSTRAINT [DF_USERMENU_IDMenu] DEFAULT (0) FOR
[USM_IDMENU]
GO

ALTER TABLE [dbo].[APP_USERMENU] ADD
	CONSTRAINT [FK_APP_USERMENU_APP_MENU] FOREIGN KEY
	(
		[USM_IDMENU]
	) REFERENCES [dbo].[APP_MENU] (
		[MNU_IDMENU]
	),
	CONSTRAINT [FK_APP_USERMENU_APP_USERS] FOREIGN KEY
	(
		[USM_USERNAME]
	) REFERENCES [dbo].[APP_USERS] (
		[USR_USERNAME]
	)
GO

ALTER TABLE [dbo].[HOSTS] ADD
	CONSTRAINT [FK_HOSTS_VLANS] FOREIGN KEY
	(
		[VLN_NAME]
	) REFERENCES [dbo].[VLANS] (
		[VLN_NAME]
	)
GO
```

```
ALTER TABLE [dbo].[PGP_CLI] ADD
	CONSTRAINT [FK_PGP_CLI_CLIENTS] FOREIGN KEY
	(
		[CLI_IP]
	) REFERENCES [dbo].[CLIENTS] (
		[CLI_IP]
	),
	CONSTRAINT [FK_PGP_CLI_PORT_GROUPS] FOREIGN KEY
	(
		[PGP_NAME]
	) REFERENCES [dbo].[PORT_GROUPS] (
		[PGP_NAME]
	)
GO

ALTER TABLE [dbo].[VGP_CLI] ADD
	CONSTRAINT [FK_VGP_CLI_CLIENTS] FOREIGN KEY
	(
		[CLI_IP]
	) REFERENCES [dbo].[CLIENTS] (
		[CLI_IP]
	),
	CONSTRAINT [FK_VGP_CLI_VLAN_GROUPS] FOREIGN KEY
	(
		[VGP_NAME]
	) REFERENCES [dbo].[VLAN_GROUPS] (
		[VGP_NAME]
	)
GO

ALTER TABLE [dbo].[VGP_PGP] ADD
	CONSTRAINT [FK_VGP_PGP_PORT_GROUPS] FOREIGN KEY
```

```
	(
		[PGP_NAME]
	) REFERENCES [dbo].[PORT_GROUPS] (
		[PGP_NAME]
	),
	CONSTRAINT [FK_VGP_PGP_VLAN_GROUPS] FOREIGN KEY
	(
		[VGP_NAME]
	) REFERENCES [dbo].[VLAN_GROUPS] (
		[VGP_NAME]
	)
GO

ALTER TABLE [dbo].[VLN_CLI] ADD
	CONSTRAINT [FK_VLN_CLI_CLIENTS] FOREIGN KEY
	(
		[CLI_IP]
	) REFERENCES [dbo].[CLIENTS] (
		[CLI_IP]
	),
	CONSTRAINT [FK_VLN_CLI_VLANS] FOREIGN KEY
	(
		[VLN_NAME]
	) REFERENCES [dbo].[VLANS] (
		[VLN_NAME]
	)
GO

ALTER TABLE [dbo].[VLN_PGP] ADD
	CONSTRAINT [FK_VLN_PGP_PORT_GROUPS] FOREIGN KEY
	(
		[PGP_NAME]
```

```
        ) REFERENCES [dbo].[PORT_GROUPS] (
                [PGP_NAME]
        ),
        CONSTRAINT [FK_VLN_PGP_VLANS] FOREIGN KEY
        (
                [VLN_NAME]
        ) REFERENCES [dbo].[VLANS] (
                [VLN_NAME]
        )
GO

ALTER TABLE [dbo].[VLN_VGP] ADD
        CONSTRAINT [FK_VLN_VGP_VLAN_GROUPS] FOREIGN KEY
        (
                [VGP_NAME]
        ) REFERENCES [dbo].[VLAN_GROUPS] (
                [VGP_NAME]
        ),
        CONSTRAINT [FK_VLN_VGP_VLANS] FOREIGN KEY
        (
                [VLN_NAME]
        ) REFERENCES [dbo].[VLANS] (
                [VLN_NAME]
        )
GO
```