A. IDENTIFICACIÓN DE ELEMENTOS DE LAS VLAN.

• BENEFICIOS DE UNA VLAN.

- • Grupos de Trabajo Virtuales
- • Reducen los costes administrativos relacionados con la resolución de los problemas asociados con los traslados, adiciones y cambios.
- • Proporcionan una actividad de difusión controlada.
- • Proporcionan seguridad de grupo de trabajo y de red.
- • Suponen un ahorro de dinero, al usar los hubs existentes

2. Rangos de ID de la VLAN.

VTP son las siglas de **VLAN Trunking Protocol**, un protocolo usado para configurar y administrar VLANs en equipos Cisco. VTP opera en 3 modos distintos: - Cliente - Servidor - Transparente

Los administradores de red solo pueden cambiar la configuración de VLANs en modo Servidor. Después de que se realiza algún cambio, estos son distribuidos a todos los demás dispositivos en el dominio VTP a través de los enlaces que permiten el Trunk. Los dispositivos que operan en modo transparente no aplican las configuraciones VLAN que reciben, ni envían las suyas a otros dispositivos, sin embargo los dispositivos en modo transparente que usan la versión 2 del protocolo VTP enviarán la información que reciban (publicaciones VTP) a otros dispositivos a los que estén conectados, actualmente (año 2009) dichas publicaciones se envían cada 5 minutos. Los dispositivos que operen en modo cliente, automáticamente aplicarán la configuración que reciban del dominio VTP, en el modo cliente NO se podrán crear VLAN, sino que sólo podrá aplicar la información que reciba de las publicaciones VTP.

Las configuraciones VTP en una red son controladas por un número de revisión. Si el número de revisión de una actualización recibida por un switch en modo cliente o servidor es más alto que la revisión anterior, entonces se aplicará la nueva configuración. De lo contrario se ignoran los cambios recibidos. Cuando se añaden nuevos dispositivos a un dominio VTP, se debe resetear los números de revisión de todo el dominio VTP para evitar conflictos. Se recomienda mucho cuidado al usar VTP cuando haya cambios de topología ya sean lógicos o físicos.

Realmente no es necesario resetear todos los números de revisión del dominio. Sólo hay que asegurarse de que los switches nuevos que se agregen al dominio VTP tengan números de revisión más bajos que los que están configurados en la red. Si no fuese así, bastaría con eliminar el nombre del dominio del switch que se agrega. Esa operación vuelve a poner a cero su contador de revisión.

El VTP permite a un administrador de red configurar un switch de modo que propagará las configuraciones de la VLAN hacia los otros switches en la red. El switch se puede configurar en la función de servidor del VTP o de cliente del VTP. El VTP sólo aprende sobre las VLAN de rango normal (ID de VLAN 1 a 1005). Las VLAN de rango extendido (ID mayor a 1005) no son admitidas por el VTP. El VTP guarda las configuraciones de la VLAN en la base de datos de la VLAN, denominada vlan.dat.

El VTP permite al administrador de red realizar cambios en un switch que está configurado como servidor del VTP. Básicamente, el servidor del VTP distribuye y sincroniza la información de la VLAN a los switches habilitados por el VTP a través de la red conmutada, lo que minimiza los problemas causados por las configuraciones incorrectas y las inconsistencias en las configuraciones. El VTP guarda las configuraciones de la VLAN en la base de datos de la VLAN denominada vlan.dat. Para que dos equipos que utilizan VTP puedan compartir información sobre VLAN, es necesario que pertenezcan al mismo dominio.

– VLAN de rango normal

A. IDENTIFICACIÓN DE ELEMENTOS DE LAS VLAN.

• BENEFICIOS DE UNA VLAN.

o • Grupos de Trabajo Virtuales o • Reducen los costes administrativos relacionados con la resolución de los problemas asociados con los

traslados, adiciones y cambios. o • Proporcionan una actividad de difusión controlada. o • Proporcionan seguridad de grupo de trabajo y de red. o • Suponen un ahorro de dinero, al usar los hubs existentes

2. Rangos de ID de la VLAN.

VTP son las siglas de VLAN Trunking Protocol, un protocolo usado para configurar y administrar VLANs en equipos Cisco. VTP opera en 3 modos distintos: - Cliente - Servidor - Transparente

Los administradores de red solo pueden cambiar la configuración de VLANs en modo Servidor. Después de que se realiza algún cambio, estos son distribuidos a todos los demás dispositivos en el dominio VTP a través de los enlaces que permiten el Trunk. Los dispositivos que operan en modo transparente no aplican las configuraciones VLAN que reciben, ni envían las suyas a otros dispositivos, sin embargo los dispositivos en modo transparente que usan la versión 2 del protocolo VTP enviarán la información que reciban (publicaciones VTP) a otros dispositivos a los que estén conectados, actualmente (año 2009) dichas publicaciones se envían cada 5 minutos. Los dispositivos que operen en modo cliente, automáticamente aplicarán la configuración que reciban del dominio VTP, en el modo cliente NO se podrán crear VLAN, sino que sólo podrá aplicar la información que reciba de las publicaciones VTP.

Las configuraciones VTP en una red son controladas por un número de revisión. Si el número de revisión de una actualización recibida por un switch en modo cliente o servidor es más alto que la revisión anterior, entonces se aplicará la nueva configuración. De lo contrario se ignoran los cambios recibidos. Cuando se añaden nuevos dispositivos a un dominio VTP, se debe resetear los números de revisión de todo el dominio VTP para evitar conflictos. Se recomienda mucho cuidado al usar VTP cuando haya cambios de topología ya sean lógicos o físicos.

Realmente no es necesario resetear todos los números de revisión del dominio. Sólo hay que asegurarse de que los switches nuevos que se agregen al dominio VTP tengan números de revisión más bajos que los que están configurados en la red. Si no fuese así, bastaría con eliminar el nombre del dominio del switch que se agrega. Esa operación vuelve a poner a cero su contador de revisión.

El VTP permite a un administrador de red configurar un switch de modo que propagará las configuraciones de la VLAN hacia los otros switches en la red. El switch se puede configurar en la función de servidor del VTP o de cliente del VTP. El VTP sólo aprende sobre las VLAN de rango normal (ID de VLAN 1 a 1005). Las VLAN de rango extendido (ID mayor a 1005) no son admitidas por el VTP. El VTP guarda las configuraciones de la VLAN en la base de datos de la VLAN, denominada vlan.dat.

El VTP permite al administrador de red realizar cambios en un switch que está configurado como servidor del VTP. Básicamente, el servidor del VTP distribuye y sincroniza la información de la VLAN a los switches habilitados por el VTP a través de la red conmutada, lo que minimiza los problemas causados por las configuraciones incorrectas y las inconsistencias en las configuraciones. El VTP guarda las configuraciones de la VLAN en la base de datos de la VLAN denominada vlan.dat. Para que dos equipos que utilizan VTP puedan compartir información sobre VLAN, es necesario que pertenezcan al mismo dominio.

– VLAN de rango normal

El VTP sólo aprende sobre las VLAN de rango normal (ID de VLAN 1 a 1005). Las VLAN de rango extendido (ID mayor a 1005) no son admitidas por el VTP. El VTP guarda las configuraciones de la VLAN en la base de datos de la VLAN, denominada vlan.dat.

– VLAN de rango extendido

El acceso a las VLAN está dividido en un rango normal o un rango extendido, las VLAN de rango normal se utilizan en redes de pequeñas y medianas empresas, se identifican por un ID de VLAN entre el 1 y 1005 y las de rango extendido posibilita a los proveedores de servicios que amplien sus infraestructuras a una cantidad de clientes mayor y se identifican mediante un ID de VLAN entre 1006 y 4094.

El protocolo de enlace troncal de la VLAN VTP (que lo veremos más adelante) sólo aprende las VLAN de rango normal y no las de rango extendido.

- **Tipos de VLAN.**

De acuerdo con la terminología común de las VLAN se clasifican en:

VLAN de Datos.- es la que está configurada sólo para enviar tráfico de datos generado por el usuario, a una VLAN de datos también se le denomina VLAN de usuario.

VLAN Predeterminada.- Es la VLAN a la cual todos los puertos del Switch se asignan cuando el dispositivo inicia, en el caso de los switches cisco por defecto es la VLAN1, otra manera de referirse a la VLAN de predeterminada es aquella que el administrador haya definido como la VLAN a la que se asignan todos los puertos cuando no estan en uso.

VLAN Nativa.- una VLAN nativa está asiganada a un puerto troncal 802.1Q, un puerto de enlace troncal 802.1Q admite el tráfico que llega de una VLAN y también el que no llega de las VLAN's, la VLAN nativa sirve como un identificador común en extremos opuestos de un elace troncal, es aconsejable no utilizar la VLAN1 como la VLAN Nativa.

VLAN de administración.- Es cualquier vlan que el administrador configura para acceder a la administración de un switch, la VLAN1 sirve por defecto como la VLAN de administración si es que no se define otra VLAN para que funcione como la VLAN de Administración.

– VLAN DE DATOS.

Una VLAN de datos es una VLAN configurada para enviar sólo tráfico de datos generado por el usuario. Una VLAN podría enviar tráfico basado en voz o tráfico utilizado para administrar el switch, pero este tráfico no sería parte de una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos. La importancia de separar los datos del usuario del tráfico de voz y del control de administración del switch se destaca mediante el uso de un término específico para identificar las VLAN que sólo pueden enviar datos del usuario: una "VLAN de datos". A veces, a una VLAN de datos se la denomina VLAN de usuario.

– VLAN PREDETERMINADA.

Todos los puertos de switch se convierten en un miembro de la VLAN predeterminada luego del arranque inicial del switch. Hacer participar a todos los puertos de switch en la VLAN predeterminada los hace a todos parte del mismo dominio de broadcast. Esto admite cualquier dispositivo conectado a cualquier puerto de switch para comunicarse con otros dispositivos en otros puertos de switch.

El VTP sólo aprende sobre las VLAN de rango normal (ID de VLAN 1 a 1005). Las VLAN de rango extendido (ID mayor a 1005) no son admitidas por el VTP. El VTP guarda las configuraciones de la VLAN

en la base de datos de la VLAN, denominada vlan.dat.

– VLAN de rango extendido

El acceso a las VLAN está dividido en un rango normal o un rango extendido, las VLAN de rango normal se utilizan en redes de pequeñas y medianas empresas, se identifican por un ID de VLAN entre el 1 y 1005 y las de rango extendido posibilita a los proveedores de servicios que amplien sus infraestructuras a una cantidad de clientes mayor y se identifican mediante un ID de VLAN entre 1006 y 4094.

El protocolo de enlace troncal de la VLAN VTP (que lo veremos más adelante) sólo aprende las VLAN de rango normal y no las de rango extendido.

• Tipos de VLAN.

De acuerdo con la terminología común de las VLAN se clasifican en:

VLAN de Datos.- es la que está configurada sólo para enviar tráfico de datos generado por el usuario, a

una VLAN de datos también se le denomina VLAN de usuario.

VLAN Predeterminada.- Es la VLAN a la cual todos los puertos del Switch se asignan cuando el

dispositivo inicia, en el caso de los switches cisco por defecto es la VLAN1, otra manera de referirse a la VLAN de predeterminada es aquella que el administrador haya definido como la VLAN a la que se asignan todos los puertos cuando no estan en uso.

VLAN Nativa.- una VLAN nativa está asiganada a un puerto troncal 802.1Q, un puerto de enlace

troncal 802.1Q admite el tráfico que llega de una VLAN y también el que no llega de las VLAN's, la VLAN nativa sirve como un identificador común en extremos opuestos de un elace troncal, es aconsejable no utilizar la VLAN1 como la VLAN Nativa.

VLAN de administración.- Es cualquier vlan que el administrador configura para acceder a la

administración de un switch, la VLAN1 sirve por defecto como la VLAN de administración si es que no se define otra VLAN para que funcione como la VLAN de Administración.

– VLAN DE DATOS. Una VLAN de datos es una VLAN configurada para enviar sólo tráfico de datos generado por el usuario. Una VLAN podría enviar tráfico basado en voz o tráfico utilizado para administrar el switch, pero este tráfico no sería parte de una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos. La importancia de separar los datos del usuario del tráfico de voz y del control de administración del switch se destaca mediante el uso de un término específico para identificar las VLAN que sólo pueden enviar datos del usuario: una "VLAN de datos". A veces, a una VLAN de datos se la denomina VLAN de usuario.

– VLAN PREDETERMINADA. Todos los puertos de switch se convierten en un miembro de la VLAN predeterminada luego del arranque inicial del switch. Hacer participar a todos los puertos de switch en la VLAN predeterminada los hace a todos parte del mismo dominio de broadcast. Esto admite cualquier dispositivo conectado a cualquier puerto de switch para comunicarse con otros dispositivos en otros puertos de switch.

– VLAN NATIVA.

La Vlan nativa es una condición usada con interfaces que son configuradas como vlan troncales (enlace troncales). Cuando un puerto del switch ha sido configurado como un enlace troncal, este es etiquetado con su respectivo identificador de número de vlan. Las tramas de todas las vlan son trasportadas por un enlace en modo troncal, por medio de la un tag que puede ser **802.1Q** o **ISL**, exceptuando a esto, las tramas que pertenecen a la vlan 1.

– VLAN DE ADMINISTRACIÓN.

Una VLAN de datos es una VLAN configurada para enviar sólo tráfico de datos generado por el usuario. Una VLAN podría enviar tráfico basado en voz o tráfico utilizado para administrar el switch, pero este tráfico no sería parte de una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos. La importancia de separar los datos del usuario del tráfico de voz y del control de administración del switch se destaca mediante el uso de un término específico para identificar las VLAN que sólo pueden enviar datos del usuario: una "VLAN de datos". A veces, a una VLAN de datos se la denomina VLAN de usuario

-VLAN DE VOZ.

Es fácil apreciar por qué se necesita una VLAN separada para admitir la Voz sobre IP (VoIP). Imagine que está recibiendo una llamada de urgencia y de repente la calidad de la transmisión se distorsiona tanto que no puede comprender lo que está diciendo la persona que llama. El tráfico de VoIP requiere:

Ancho de banda garantizado para asegurar la calidad de la voz

¨ Prioridad de la transmisión sobre los tipos de tráfico de la red

¨ Capacidad para ser enrutado en áreas congestionadas de la red

¨ Demora de menos de 150 milisegundos (ms) a través de la red

- **Modos de membresía de los puertos switch de VLAN.**

- **Enlace troncal de la VLAN.**

Un enlace troncal es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN. Un enlace troncal de VLAN le permite extender las VLAN a través de toda una red. Cisco admite IEEE 802.1Q para la coordinación de enlaces troncales en interfaces Fast Ethernet y Gigabit Ethernet. Más adelante en esta sección, aprenderá acerca de 802.1Q. Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre switches y routers.

- **Etiquetado de trama 802.1Q**

Los switches son dispositivos de capa 2. Sólo utilizan la información del encabezado de trama de Ethernet para enviar paquetes. El encabezado de trama no contiene la información que

– VLAN NATIVA.

La Vlan nativa es una condición usada con interfaces que son configuradas como vlan troncales (enlace

troncales). Cuando un puerto del switch ha sido configurado como un enlace troncal, este es etiquetado con su respectivo identificador de número de vlan. Las tramas de todas las vlan son trasportadas por un enlace en modo troncal, por medio de la un tag que puede ser 802.1Q o ISL, exceptuando a esto, las tramas que pertenecen a la vlan 1.

– VLAN DE ADMINISTRACIÓN.

Una VLAN de datos es una VLAN configurada para enviar sólo tráfico de datos generado por el usuario. Una VLAN podría enviar tráfico basado en voz o tráfico utilizado para administrar el switch, pero este tráfico no sería parte de una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos. La importancia de separar los datos del usuario del tráfico de voz y del control de administración del switch se destaca mediante el uso de un término específico para identificar las VLAN que sólo pueden enviar datos del usuario: una "VLAN de datos". A veces, a una VLAN de datos se la denomina VLAN de usuario

-VLAN DE VOZ. Es fácil apreciar por qué se necesita una VLAN separada para admitir la Voz sobre IP (VoIP). Imagine que está recibiendo una llamada de urgencia y de repente la calidad de la transmisión se distorsiona tanto que no puede comprender lo que está diciendo la persona que llama. El tráfico de VoIP requiere:

Ancho de banda garantizado para asegurar la calidad de la voz

¨ Prioridad de la transmisión sobre los tipos de tráfico de la red

¨ Capacidad para ser enrutado en áreas congestionadas de la red

¨ Demora de menos de 150 milisegundos (ms) a través de la red

• Modos de membresía de los puertos switch de VLAN.

• Enlace troncal de la VLAN.

Un enlace troncal es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN. Un enlace troncal de VLAN le permite extender las VLAN a través de toda una red. Cisco admite IEEE 802.1Q para la coordinación de enlaces troncales en interfaces Fast Ethernet y Gigabit Ethernet. Más adelante en esta sección, aprenderá acerca de 802.1Q. Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre switches y routers.

• Etiquetado de trama 802.1Q

Los switches son dispositivos de capa 2. Sólo utilizan la información del encabezado de trama de Ethernet para enviar paquetes. El encabezado de trama no contiene la información que

indique a qué VLAN pertenece la trama. Posteriormente, cuando las tramas de Ethernet se ubican en un enlace troncal, necesitan información adicional sobre las VLAN a las que pertenecen. Esto se logra por medio de la utilización del encabezado de encapsulación 802.1Q. Este encabezado agrega una etiqueta a la trama de Ethernet original y especifica la VLAN a la que pertenece la trama.

- **VLAN nativas y enlace troncal 802.1Q**

Un enlace troncal es un enlace punto a punto entre dos sispositivos de red, el cual transporta más de una vlan. Un enlace troncal de VLAN no pertence a una VLAN específica, sino que es un conducto para las VLAN entre switches y routers.

Existen deiferentes modos de enlaces troncales como el 802.1Q y el ISL, en la actualidad sólo se usa el 802.1Q, dado que el ISL es utilizado por las redes antiguas, un puerto de enlace troncal IEEE 802.1Q admite tráfico etiquetado y sin etiquetar, el enlace troncal dinámico DTP es un protocolo propiedad de cisco, DTP administra la negociación del enlace troncal sólo si el puerto en el otro switch se configura en modo de enlace troncal que admita DTP.

Configuración de un enlace troncal 802.1Q en un Switch:

```
Ciscoredes# configure terminal
Ciscoredes(config)# interface interface-id
Ciscoredes(config-if)# switchport mode trunk
Ciscoredes(config-if)# switchport trunk native vlan vlan-id
Ciscoredes(config-if)# exit
```

Donde:

- interface .- Comando para entrar al modo de configuración de interfaz.
- Interface-id.- Tipo de puerto a configurar por ejemplo fastethernet 0/0
- Switchport mode trunk .- Definir que el enlace que conecta a los switches sea un enlace troncal
- Switchport trunk native vlan vlan-id .- Especificar otra VLAN como la VLAN nativa para los enlaces troncales.

- **Puerto de acceso en los switch.**

Después de que un puerto ha sido asignado a una VLAN, a través de ese puerto no se puede enviar ni recibir datos desde dispositivos incluidos en otra VLAN sin la intervención de algún dispositivo de capa 3.

El dispositivo que se conecta a un puerto, posiblemente no tenga conocimiento de la existencia de la VLAN a la que pertenece dicho puerto. El dispositivo simplemente sabe que es miembro de una sub-red y que puede ser capaz de hablar con otros miembros de la sub-red simplemente enviando información al segmento cableado. El switch es responsable de identificar que la información viene de una VLAN determinada y de asegurarse de que esa información llega a todos los demás miembros de la VLAN. El switch también se asegura de que el resto de puertos que no están en dicha VLAN no reciben dicha información.

Este planteamiento es sencillo, rápido y fácil de administrar, dado que no hay complejas tablas en las que mirar para configurar la segmentación de la VLAN. Si la asociación de puerto-a-VLAN se hace con un ASIC (acrónimo en inglés de Application-Specific

indique a qué VLAN pertenece la trama. Posteriormente, cuando las tramas de Ethernet se ubican en un enlace troncal, necesitan información adicional sobre las VLAN a las que pertenecen. Esto se logra por

medio de la utilización del encabezado de encapsulación 802.1Q. Este encabezado agrega una etiqueta a la trama de Ethernet original y especifica la VLAN a la que pertenece la trama.

• VLAN nativas y enlace troncal 802.1Q

Un enlace troncal es un enlace punto a punto entre dos sispositivos de red, el cual transporta más de una vlan. Un enlace troncal de VLAN no pertence a una VLAN específica, sino que es un conducto para las VLAN entre switches y

routers.

Existen deiferentes modos de enlaces troncales como el 802.1Q y el ISL, en la actualidad sólo se usa el 802.1Q, dado

que el ISL es utilizado por las redes antiguas, un puerto de enlace troncal IEEE 802.1Q admite tráfico etiquetado y sin etiquetar, el enlace troncal dinámico DTP es un protocolo propiedad de cisco, DTP administra la negociación del enlace troncal sólo si el puerto en el otro switch se configura en modo de enlace troncal que admita DTP.

Configuración de un enlace troncal 802.1Q en un Switch:

Ciscoredes# configure terminal Ciscoredes(config)# interface interface-id Ciscoredes(config-if)# switchport mode trunk Ciscoredes(config-if)# switchport trunk native vlan vlan-id Ciscoredes(config-if)# exit

Donde:

• interface .- Comando para entrar al modo de configuración de interfaz.

• Interface-id.- Tipo de puerto a configurar por ejemplo fastethernet 0/0

• Switchport mode trunk .- Definir que el enlace que conecta a los switches sea un enlace troncal

• Switchport trunk native vlan vlan-id .- Especificar otra VLAN como la VLAN nativa para los enlaces troncales.

• Puerto de acceso en los switch. Después de que un puerto ha sido asignado a una VLAN, a través de ese puerto no se puede enviar ni recibir datos desde dispositivos incluidos en otra VLAN sin la intervención de algún dispositivo de capa 3.

El dispositivo que se conecta a un puerto, posiblemente no tenga conocimiento de la existencia de la VLAN a la que pertenece dicho puerto. El dispositivo simplemente sabe que es miembro de una sub-red y que puede ser capaz de hablar con otros miembros de la sub-red simplemente enviando información al segmento cableado. El switch es responsable de identificar que la información viene de una VLAN determinada y de asegurarse de que esa información llega a todos los demás miembros de la VLAN. El switch también se asegura de que el resto de puertos que no están en dicha VLAN no reciben dicha información.

Este planteamiento es sencillo, rápido y fácil de administrar, dado que no hay complejas tablas en las que mirar para configurar la segmentación de la VLAN. Si la asociación de puerto-a-VLAN se hace con un ASIC (acrónimo en inglés de Application-Specific

Integrated Circuit o Circuito integrado para una aplicación específica), el rendimiento es muy bueno. Un ASIC permite el mapeo de puerto-a-VLAN sea hecho a nivel hardware

- **Puerto de enlace troncal en los switch.**

- **B. CONFIGURACIÓN DE UNA VLAN.**

- **Agregar una VLAN.**

```
Ciscoredes# configure terminal
Ciscoredes(config)# vlan vlan-id
Ciscoredes(config-vlan)# name nombre-de-vlan
Ciscoredes(config-vlan)# exit
```

- Vlan .- comando para asignar las VLAN
- Valn-id.- Numero de vlan que se creará que va de un rango normal de 1-1005 (los ID 1002-1005 se reservan para Token Ring y FDDI).
- Name.- comando para especificar el nombre de la VLAN
- Nombre-de-vlan.- Nombre asignado a la VLAN, sino se asigna ningún nombre, dicho nombre será rellenado con ceros, por ejemplo para la VLAN 20 sería VLAN0020.

- **Asignación de un puerto de switch.**

Con las VLAN con pertenencia basada en el puerto de conexión del switch, el puerto asignado a la VLAN es independiente del usuario o dispositivo conectado en el puerto. Esto significa que todos los usuarios que se conectan al puerto serán miembros de la misma VLAN. Habitualmente es el administrador de la red el que realiza las asignaciones a la VLAN. Después de que un puerto ha sido asignado a una VLAN, a través de ese puerto no se puede enviar ni recibir datos desde dispositivos incluidos en otra VLAN sin la intervención de algún dispositivo de capa 3.

- **Asignación de rangos de puertos.**

En caso de tener que asignar un puerto a una aplicación, si no se elige el correspondiente "Well-Known" debe seleccionarse un número en el rango 1024 - 65535. En los sistemas Linux la asignación de puertos se encuentra en el fichero /etc/services. También pueden inspeccionarse los puertos abiertos por las distintas aplicaciones mediante la utilidad netstat.

Puede consultarse en RFC 1700 (www.faqs.org/rfcs) y en la propia IANA www.iana.org/assignments/port-numbers.

En los sistemas POSIX, los números de puertos y nombres de los servicios correspondientes, están definidos en el fichero /etc/services. En los sistemas Windows estos valores se encuentran en el fichero c:\windows\system32\drivers\etc\services, cuyo contenido, para un sistema WindowsXP. La tabla adjunta muestra algunos de estos puertos y los servicios correspondientes.

N. de puerto	Descripción

Integrated Circuit o Circuito integrado para una aplicación específica), el rendimiento es

muy bueno. Un ASIC permite el mapeo de puerto-a-VLAN sea hecho a nivel hardware

• Puerto de enlace troncal en los switch.

• B. CONFIGURACIÓN DE UNA VLAN.

• Agregar una VLAN.

Ciscoredes# configure terminal Ciscoredes(config)# vlan vlan-id Ciscoredes(config-vlan)# name nombre-de-vlan Ciscoredes(config-vlan)# exit

• Vlan .- comando para asignar las VLAN

• Valn-id.- Numero de vlan que se creará que va de un rango normal de 1-1005 (los ID 1002-1005 se reservan para Token Ring y FDDI).

• Name.- comando para especificar el nombre de la VLAN

• Nombre-de-vlan.- Nombre asignado a la VLAN, sino se asigna ningún nombre, dicho nombre será rellenado con ceros, por ejemplo para la VLAN 20 sería VLAN0020.

• Asignación de un puerto de switch. Con las VLAN con pertenencia basada en el puerto de conexión del switch, el puerto asignado a la VLAN es independiente del usuario o dispositivo conectado en el puerto. Esto significa que todos los usuarios que se conectan al puerto serán miembros de la misma VLAN. Habitualmente es el administrador de la red el que realiza las asignaciones a la VLAN. Después de que un puerto ha sido asignado a una VLAN, a través de ese puerto no se puede enviar ni recibir datos desde dispositivos incluidos en otra VLAN sin la intervención de algún dispositivo de capa 3.

• Asignación de rangos de puertos.

En caso de tener que asignar un puerto a una aplicación, si no se elige el correspondiente "Well-Known" debe seleccionarse un número en el rango 1024 - 65535. En los sistemas Linux la asignación de puertos se encuentra en el fichero /etc/services. También pueden inspeccionarse los puertos abiertos por las distintas aplicaciones mediante la utilidad netstat.

Puede consultarse en RFC 1700 (www.faqs.org/rfcs) y en la propia IANA www.iana.org/assignments/port-numbers.

En los sistemas POSIX, los números de puertos y nombres de los servicios correspondientes, están definidos en el fichero /etc/services. En los sistemas Windows estos valores se encuentran en el fichero c:\windows\system32\drivers\etc\services, cuyo contenido, para un sistema WindowsXP. La tabla adjunta muestra algunos de estos puertos y los servicios correspondientes.

N. de puerto Descripción

0	Reservado
1	**TCP** Servicio de multiplexado de puertos (TCPMUX)
4	No asignado
5	**RJE** ("Remote Job Entry")
6	No asignado
7	ECHO
18	**MSP** ("Message Send Protocol")
20	**FTP** ("File Transfer Protocol" Ap. C) Datos
21	**FTP** ("File Transfer Protocol") Control
22	**SSH** Secure Shell Remote Login Protocol
23	**Telnet** (acceso a terminal remoto Ap. C y 8.7)
25	**SMTP** ("Simple Mail Transfer Protocol")
29	**MSG ICP**
37	Time
42	Host Name Server (Nameserv)
43	**Whois**
49	Login Host Protocol (Login)
53	**DNS** ("Domain Name System")
59	IDENT
69	**TFTP** ("Trivial File Transfer Protocol")
70	Servicio **Gopher** (Ap. C)
79	Servicio **Finger** (N-13)
80	**WWW-HTTP** ("Hyper Text Transfer Protocol" Ap. C)
103	X.400 Standard

0 Reservado

1 TCP Servicio de multiplexado de puertos (TCPMUX)

4 No asignado

5 RJE ("Remote Job Entry")

6 No asignado

7 ECHO

18 MSP ("Message Send Protocol")

20 FTP ("File Transfer Protocol" Ap. G) Datos

21 FTP ("File Transfer Protocol") Control

22 SSH Secure Shell Remote Login Protocol

23 Telnet (acceso a terminal remoto Ap. G y 8.7)

25 SMTP ("Simple Mail Transfer Protocol")

29 MSG ICP

37 Time

42 Host Name Server (Nameserv)

43 Whois

49 Login Host Protocol (Login)

53 DNS ("Domain Name System")

59 IDENT

69 TFTP ("Trivial File Transfer Protocol")

70 Servicio Gopher (Ap. G)

79 Servicio Finger (N-13)

80 WWW-HTTP ("Hyper Text Transfer Protocol" Ap. G)

103 X.400 Standard

108	SNA Gateway Access Server
109	**POP2** ("Post Office Protocol")
110	**POP3** ("Post Office Protocol")
111	SUN-**RPC**. ("Remote Procedure Call")
113	**UDP** ("User Datagram Protocol" RFC-768)
115	**SFTP** ("Simple File Transfer Protocol")
118	Servicios SQL
119	**NNTP** ("Network News Transfer Protocol" Ap. C)
137	netbios-ns NETBIOS Name Service
138	netbios-dgm NetBIOS Datagram Service
139	netbios-ssn NetBIOS Session Service
143	**IMAP** ("Interim Mail Access Protocol")
156	SQL Server
161	**SNMP** ("Simple Network Management Protocol")
162	**SNMP** trap
179	**BGP** ("Border Gateway Patrol")
190	**GACP** ("Gateway Access Control Protocol")
194	**IRC** ("Internet Relay Chat")
197	**DLS** ("Directory Location Service")
210	wais (servicio de búsquedas Ap. C)
389	**LDAP** ("Lightweight Directory Access Protocol")
396	Novell Netware sobre IP
443	**HTTPS** ("HyperText Transfer Protocol" Ap. C)
444	**SNNP** ("Simple Network Paging Protocol")

108 SNA Gateway Access Server

109 POP2 ("Post Office Protocol")

110 POP3 ("Post Office Protocol")

111 SUN-RPC. ("Remote Procedure Call")

113 UDP ("User Datagram Protocol" RFC-768)

115 SFTP ("Simple File Transfer Protocol")

118 Servicios SQL

119 NNTP ("Network News Transfer Protocol" Ap. G)

137 netbios-ns NETBIOS Name Service

138 netbios-dgm NetBIOS Datagram Service

139 netbios-ssn NetBIOS Session Service

143 IMAP ("Interim Mail Access Protocol")

156 SQL Server

161 SNMP ("Simple Network Management Protocol")

162 SNMP trap

179 BGP ("Border Gateway Patrol")

190 GACP ("Gateway Access Control Protocol")

194 IRC ("Internet Relay Chat")

197 DLS ("Directory Location Service")

210 wais (servicio de búsquedas Ap. G)

389 LDAP ("Lightweight Directory Access Protocol")

396 Novell Netware sobre IP

443 HTTPS ("HyperText Transfer Protocol" Ap. G)

444 SNNP ("Simple Network Paging Protocol")

El

445	Microsoft-DS
458	Apple QuickTime
513	**rlogin** Acceso remoto
546	**DHCP** ("Dynamic Host Configuration Protocol" A3.6) Cliente
547	**DHCP** Servidor
563	SNEWS
569	MSN
631	**UDP** ("User Datagram Protocol")
1080	Socks Proxy
Otros puertos no estándar	
1503	T.120 Utilizado por aplicaciones que comparten aplicaciones
1720	H.323 Utilizado para escuchar llamadas entrantes por aplicaciones como VideoLink_Pro de Smith Micro y Microsoft NetMeeting.
1723	**PPTP** ("Point-to-Point Tunneling Protocol")
2049	**NFS.**
6660-6669	**TCP** ("Transmission Control Protocol")
8080	Web proxy caching service

- **C. ADMINISTRACIÓN DE LAS VLAN.**
- **Verificación de las vinculaciones de puerto y de las VLAN.**
  - **Vínculos al puerto de administración.**
  - **Administración de la pertenencia al puerto.**

445 Microsoft-DS

458 Apple QuickTime

513 rlogin Acceso remoto

546 DHCP ("Dynamic Host Configuration Protocol" A3.6) Cliente

547 DHCP Servidor

563 SNEWS

569 MSN

631 UDP ("User Datagram Protocol")

1080 Socks Proxy

Otros puertos no estándar

1503 T.120 Utilizado por aplicaciones que comparten aplicaciones

1720

H.323 Utilizado para escuchar llamadas entrantes por aplicaciones como VideoLink_Pro de Smith Micro y Microsoft NetMeeting.

1723 PPTP ("Point-to-Point Tunneling Protocol")

2049 NFS.

6660-6669 TCP ("Transmission Control Protocol")

8080 Web proxy caching service

• C. ADMINISTRACIÓN DE LAS VLAN.

• Verificación de las vinculaciones de puerto y de las VLAN.

• Vínculos al puerto de administración.

• Administración de la pertenencia al puerto.

1 È