INSTITUTO POLITECNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERIA MECANICA Y ELECTRICA UNIDAD CULHUACAN

SEMINARIO DE TITULACION

"INTERCONECTIVIDAD Y SEGMENTACION EN REDES DE ALTA VELOCIDAD"

TESINA

"IMPLEMENTACIÓN DE GRUPOS DE TRABAJO POR MEDIO DE VLAN"

QUE PRESENTAN PARA OBTENER EL TITULO DE **INGENIERO EN COMPUTACIÓN**

Hernández Flores Héctor
Trujano Martínez Luis Alberto

INGENIERO EN COMUNICACIONES Y ELECTRONICA

Fabián Martínez Oscar Manuel
Rodríguez Jacuinde Oscar

ASESORES:

M. EN C. RAYMUNDO SANTANA ALQUICIRA

VIGENCIA: DES/ESIME-CUL/5052005/22/11

México D. F., Febrero 2012.

INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE INGENIERIA MECANICA Y ELECTRICA
UNIDAD CULHUACAN

TESINA

QUE PARA OBTENER EL TITULO DE: **INGENIERO EN COMPUTACIÓN**

NOMBRE DEL SEMINARIO: “INTERCONECTIVIDAD Y SEGMENTACION EN REDES DE ALTA VELOCIDAD”

VIGENCIA: DES/ESIME-CUL/5052005/22/11

QUE DEBERAN DESARROLLAR:

Hernández Flores Héctor
Trujano Martínez Luis Alberto

Y QUE PARA OBTENER EL TITULO DE: **INGENIERO EN COMUNICAIONES Y ELECTRONICA**

DEBERAN DESARROLLAR:

Fabián Martínez Oscar Manuel
Rodríguez Jacuinde Oscar

“IMPLEMENTACIÓN DE GRUPOS DE TRABAJO POR MEDIO DE VLAN”

Una VLAN (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física. Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, limitaciones de dirección, etc.), ya que se define una segmentación lógica basada en el agrupamiento de equipos según determinados criterios (direcciones MAC, número de puertos, protocolo, etc.).
.

CAPITULADO

México D. F., Febrero de 2012.

M. en C. RAYMUNDO SANTANA ALQUICIRA
Coordinador del Seminario

DR. JOSÉ VELÁZQUEZ LÓPEZ
Jefe de la carrera de I.C.

AGRADECIMIENTOS

Está tesis está dedicada a todas aquellas personas que me han ayudado, apoyado y comprendido todo este tiempo, pero en especial esta dedicada a mis **Tíos**, ya que sin ellos no hubiera podido salir adelante, de todo corazón les agradezco todo lo que han hecho por mí.

Agradezco a mi **Esposa** por todo su apoyo incondicional que me brindo durante todo este proceso.

Agradezco a **Dios** por dejarme vivir esta etapa de mi vida, que ha sido llena de dicha junto con todas las personas que me rodean, y nos ha llenado de bendiciones.

Agradezco a todos mis **Amigos** que me han acompañado y apoyado a lo largo de todo este proceso.

Agradezco a todos mis **Profesores** por todo su tiempo y dedicación que me han dedicado.

Fabián Martínez Oscar Manuel

Un sincero agradecimiento por el respaldo incondicional de mis padres Francisco Hernández López, Magdalena Flores Pérez y hermanos, sin los cuales hubiera sido más difícil este proyecto de vida. Por tal motivo éste reconocimiento también es de ellos.

Durante el proceso de mi formación académica han sido muchas los profesores e instituciones a las que quiero expresar mi gratitud por la enseñanza y el apoyo que me han brindado.

Quiero ofrecer un reconocimiento a todos y cada uno de mis compañeros y amigos, los cuales son muchos para enumerarlos, les agradezco por permitirme compartir nuevas experiencias a su lado así como su ayuda y enseñanza.

Hernández Flores Héctor

Quiero agradecer antes que a nadie a **Dios** por que en todos aquellos momentos difíciles siempre ha estado ahí para darme las fuerzas y sabiduría para tomar las mejores decisiones en mi vida.

Agradezco a mis **Padres** quienes educaron y formaron siempre para dar lo mejor de mí a todas las personas que me rodean. Por apoyarme y cuidarme tanto tiempo sin esperar nada más que convertirme en una persona respetable, así como a toda mi **Familia** que me han dado diferentes lecciones que siempre estarán en mi vida.

Agradezco a mis **Amigos** por todos aquellos momentos que compartimos, desde una coca comunitaria hasta partidos en las canchas como proyectos escolares que nos demostraron que siempre el trabajo en equipo será el que mejores resultados da.

Agradezco a todas las personas que han entrado y salido de mi vida, de quienes he aprendido muchas cosas y que siempre recordaré, y por todo el apoyo proporcionado en esos momentos de mi vida.

Rodríguez Jacuinde Oscar

Agradezco a dios ya mis padres por darme la oportunidad de existir, de ayudarme a crecer y guiarme en todo mi recorrido para alcanzar cada una de mis metas, aunque muchas de estas fueran difíciles de alcanzar.

Agradezco a mis hermanos que siempre han estado a mi lado brindándome todo su apoyo cuando lo necesito, por compartir conmigo los momentos felices, pero también los momentos difíciles, para hacerlos más llevaderos y poder salir adelante.

Agradezco a mi familia en general que son el motor que me mueve y me inspira para luchar cada día, ya que para mí es lo más grande que he tenido.

A todos les dedico, de la manera más sincera este logro de haber alcanzado esta meta que sin su apoyo amor y comprensión no podría haber sido posible.

Trujano Martínez Luis Alberto

ÍNDICE

INTRODUCCIÓN

INTRODUCCIÓN

No existe la menor duda que el avance de las tecnologías y de los medios de transporte, han permitido que cada día el mundo sea más accesible. Las nuevas características de los mercados financieros, las Tecnologías de la Información y Telecomunicaciones permiten que los principales mercados financieros y bursátiles del mundo se comuniquen en forma instantánea y que los operadores puedan efectuar sus operaciones como si estuvieran en los recintos y con la seguridad que le ofrecen las Telecomunicaciones.

Conforme transcurren los años el mundo de las Telecomunicaciones y de las Tecnologías de Información cobra mayor importancia para las sociedades a nivel mundial, esto es mejorando la calidad de vida, mejorando los procesos de trabajo, ahorrando costos inmensos a las empresas y también facilitando el flujo de información llegando a tal grado que no importa que tan lejos estés, ni en qué país estés, sólo importa que puedas acceder al mundo de la información.

El desarrollo de las telecomunicaciones no se va a detener, en México apenas hemos visto la punta del iceberg, las comunicaciones convergentes, la comunicación inalámbrica móvil y el Internet / e-business son un campo

Inmenso de trabajo y las personas que estén preparadas para contribuir a este desarrollo serán quienes puedan tener mayores oportunidades de trabajo.

Disminuir la brecha digital se ha convertido en uno de los objetivos principales de muchos gobiernos y organizaciones multilaterales. Si reconocemos que el Internet es la forma más efectiva de transmitir información, y compartir conocimientos jamás inventados, y una gran manera de aumentar productividad y calidad de vida, vemos porque es imperativo que las comunidades más pobres hagan todos los esfuerzos necesarios para reducir esa brecha digital.

En el clima actual de los negocios, el tener una red de computadoras confiable para comunicarse es tan importante como tener un suministro de energía eléctrica en el que se pueda confiar, por lo tanto es el fundamento de cualquier sistema de información, en el cual uno se pueda apoyar para realizar diferentes tareas de manera más compartida y segura.

Las redes de computadoras son fundamentales para el desarrollo de cualquier organización, siempre que se tengan recursos escasos o que por su naturaleza deban utilizarse de manera compartida, acortando tiempos y disminuyendo costos; de ahí la importancia de su estudio en cualquier programa relacionado con tecnología de cómputo.

Las redes en general, consisten en "compartir recursos", y uno de sus objetivos es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a 1000 km de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente.

Otro de sus múltiples beneficios consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. Por ejemplo todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias. Además, la presencia de múltiples CPU significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque se tenga un rendimiento global menor

Hoy en la actualidad las naciones compiten por recursos escasos. Antes eran todos los naturales, pero hoy compiten por otros, como las inversiones, los mercados y la gente capacitada. Hasta hace pocos años se podía disponer de la exclusividad de los recursos naturales al cerrar las fronteras. La globalización no solo ha hecho que desaparezca una buena proporción de ese tipo de barreras sino que también ha facilitado la difusión de la información y conocimientos, la cual ha generalizado la distinción de dos tipos de ventajas: La comparativa y la competitiva.

Las primeras las da la naturaleza y merece un trato muy cuidadoso. Las competitivas se obtienen poniendo en juego todas las destrezas, conocimientos y habilidades que sea capaz de desarrollar.

CAPITULO 1

REDES DE COMPUTADORA

CAPITULO 1. REDES DE COMPUTADORAS

Las redes de computadoras en general, consisten en "compartir recursos", y uno de sus objetivo es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a 1000 km de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente.

Un segundo objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. Por ejemplo todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias. Además, la presencia de múltiples CPU significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque se tenga un rendimiento global menor.

Otro objetivo es el ahorro económico. Los ordenadores pequeños tienen una mejor relación costo / rendimiento, comparada con la ofrecida por las máquinas grandes.

Estas son, a grandes rasgos, diez veces mas rápidas que el mas rápido de los microprocesadores, pero su costo es miles de veces mayor.

Este desequilibrio ha ocasionado que muchos diseñadores de sistemas construyan sistemas constituidos por poderosos ordenadores personales, uno por usuario, con los datos guardados una o mas máquinas que funcionan como servidor de archivo compartido.

Este objetivo conduce al concepto de redes con varios ordenadores en el mismo edificio. A este tipo de red se le denomina LAN (red de área local), en contraste con lo extenso de una WAN (red de área extendida), a la que también se conoce como red de gran alcance.

Un punto muy relacionado es la capacidad para aumentar el rendimiento del sistema en forma gradual a medida que crece la carga, simplemente añadiendo más procesadores. Con máquinas grandes, cuando el sistema está lleno, deberá reemplazarse con uno más grande, operación que por lo normal genera un gran gasto y una perturbación inclusive mayor al trabajo de los usuarios.

Otro objetivo del establecimiento de una red de ordenadores, es que puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre sí.

Con el ejemplo de una red es relativamente fácil para dos o más personas que viven en lugares separados, escribir informes juntos. Cuando un autor hace un cambio inmediato, en lugar de esperar varios días para recibirlos por carta. Esta rapidez hace que la cooperación entre grupos de individuos que se encuentran alejados, y que anteriormente había sido imposible de establecer, pueda realizarse ahora.

1.1 Estructura de una red

En toda red existe una colección de máquinas para correr programas de usuario (aplicaciones). Seguiremos la terminología de una de las primeras redes, denominada ARPANET, y llamaremos host a las máquinas antes mencionadas.

También, en algunas ocasiones se utiliza el término sistema terminal o sistema final. Los host están conectados mediante una subred de comunicación, o simplemente subred. El trabajo de la subred consiste en enviar mensajes entre host, de la misma manera como el sistema telefónico envía palabras entre la persona que habla y la que escucha.

El diseño completo de la red simplifica notablemente cuando se separan los aspectos puros de comunicación de la red (la subred), de los aspectos de aplicación (los host).Una subred en la mayor parte de las redes de área extendida consiste de dos componentes diferentes: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión (conocidas como circuitos, canales o troncales), se encargan de mover bits entre máquinas. Los elementos de conmutación son ordenadores especializados que se utilizan para conectar dos o más líneas de de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación deberá seleccionar una línea de salida para reexpedirlos.

1.2 Redes de área local (LAN)

Red de Area Local (LAN) como forma de normalizar las conexiones entre las máquinas que se utilizan como sistemas ofimáticos. Como su propio nombre indica, constituye una forma de interconectar una serie de equipos informáticos en una oficina. A su nivel más elemental, una LAN no es más que un medio compartido (como un cable coaxial al que se conectan todas las computadoras y las impresoras) junto con una serie de reglas que rigen el acceso a dicho medio.

La LAN más difundida, la Ethernet, utiliza un mecanismo denominado Call Sense Multiple Access-Collision Detect (CSMS-CD). Esto significa que cada equipo conectado sólo puede utilizar el cable cuando ningún otro equipo lo está utilizando.

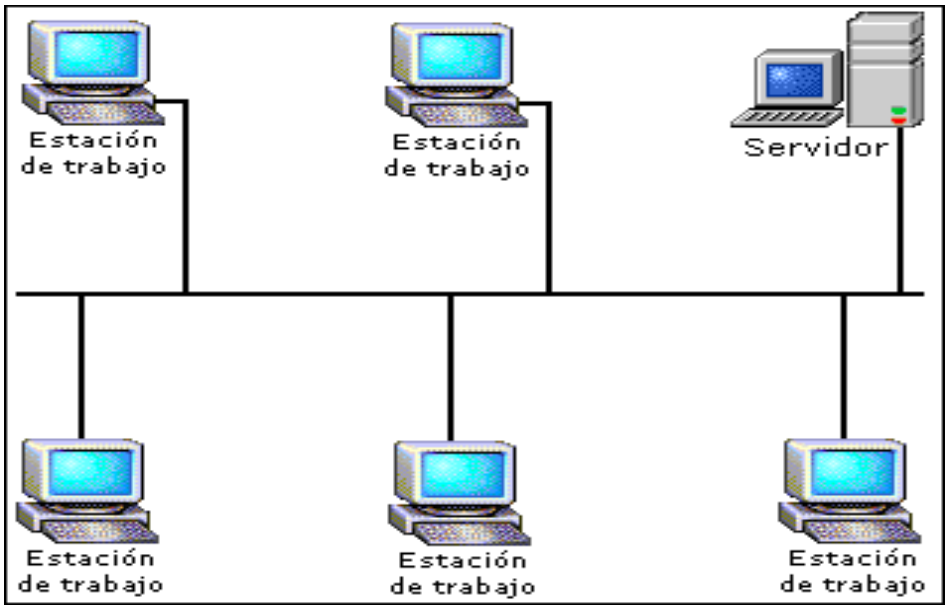


Figura 1.1 Red LAN

Si hay algún conflicto, el equipo que está intentando establecer la conexión la anula y efectúa un nuevo intento más adelante. La Ethernet transfiere datos a 10 Mbits/seg, lo suficientemente rápido como para hacer inapreciable la distancia entre los diversos equipos y dar la impresión de que están conectados directamente a su destino. Ethernet y CSMA-CD son dos ejemplos de LAN. Hay tipologías muy diversas (bus, estrella, anillo) y diferentes protocolos de acceso.

1.3 Redes de área extensa (WAN)

Cuando se llega a un cierto punto deja de ser poco práctico seguir ampliando una LAN. A veces esto viene impuesto por limitaciones físicas, aunque suele haber formas más adecuadas o económicas de ampliar una red de computadoras. Dos de los componentes importantes de cualquier red son la red de teléfono y la de datos. Son enlaces para grandes distancias que amplían la LAN hasta convertirla en una red de área extensa (WAN). Casi todos los operadores de redes nacionales ofrecen servicios para interconectar redes de computadoras, que van desde los enlaces de datos sencillos y a baja velocidad que funcionan basándose en la red pública de telefonía hasta los complejos servicios de alta velocidad (como Frame Relay) adecuados para la interconexión de las LAN.

Estos servicios de datos a alta velocidad suelen denominarse conexiones de banda ancha. Se prevé que proporcionen los enlaces necesarios entre LAN para hacer posible lo que han dado en llamarse autopistas de la información.

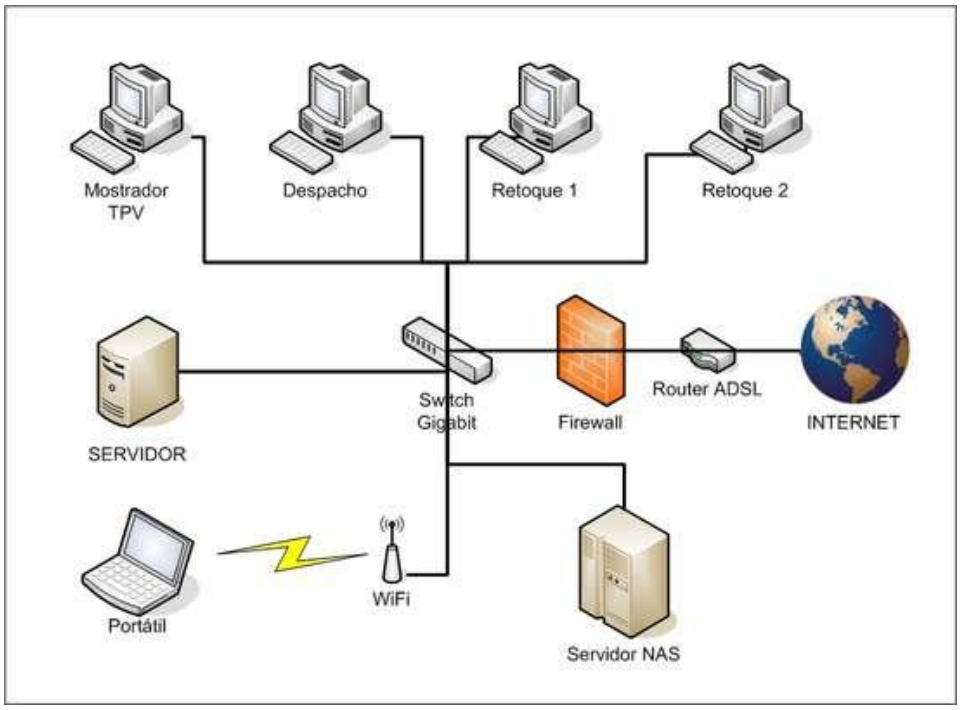


Figura 1.2 Red WAN

1.4 Routers y bridges

Los servicios en la mayoría de las LAN son muy potentes. La mayoría de las organizaciones no desean encontrarse con núcleos aislados de utilidades informáticas.

Por lo general prefieren difundir dichos servicios por una zona más amplia, de manera que los grupos puedan trabajar independientemente de su ubicación. Los routers y los bridges son equipos especiales que permiten conectar dos o más LAN. El bridge es el equipo más elemental y sólo permite conectar varias LAN de un mismo tipo.

El router es un elemento más inteligente y posibilita la interconexión de diferentes tipos de redes de ordenadores. Las grandes empresas disponen de redes corporativas de datos basadas en una serie de redes LAN y routers. Desde el punto de vista del usuario, este enfoque proporciona una red físicamente heterogénea con aspecto de un recurso homogéneo.

Proceso distribuido:

Parece lógico suponer que las computadoras podrán trabajar en conjunto cuando dispongan de la conexión de banda ancha. ¿Cómo conseguir, sin embargo, que computadoras de diferentes fabricantes en distintos países funcionen en común a través de todo el mundo? Hasta hace poco, la mayoría de las computadoras disponían de sus propias interfaces y presentaban su estructura particular. Un equipo podía comunicarse con otro de su misma familia, pero tenía grandes dificultades para hacerlo con un extraño. Sólo los más privilegiados disponían del tiempo, conocimientos y equipos necesarios para extraer de diferentes recursos informáticos aquello que necesitaban.

Los principales componentes son:

Cliente/servidor

En vez de construir sistemas informáticos como elementos monolíticos, existe el acuerdo general de construirlos como sistemas cliente/servidor. El cliente (un usuario de PC) solicita un servicio (como imprimir) que un servidor le proporciona (un procesador conectado a la LAN). Este enfoque común de la estructura de los sistemas informáticos se traduce en una separación de las funciones que anteriormente forman un todo. Los detalles de la realización van desde los planteamientos sencillos hasta la posibilidad real de manejar todos los ordenadores de modo uniforme.

1.5 Encapsulamiento

El encapsulamiento es el proceso el cual los datos que se deben enviar a través de una red se deben colocar en paquetes que se puedan administrar y rastrear. Las tres capas superiores del modelo OSI (aplicación, presentación y sesión) preparan los datos para su transmisión creando un formato común para la transmisión.

La capa de transporte divide los datos en unidades de un tamaño que se pueda administrar, denominadas segmentos.

También asigna números de secuencia a los segmentos para asegurarse de que los hosts receptores vuelvan a unir los datos en el orden correcto.

Luego la capa de red encapsula el segmento creando un paquete. Le agrega al paquete una dirección de red destino y origen, por lo general IP. En la capa de enlace de datos continúa el encapsulamiento del paquete, con la creación de una trama. Le agrega a la trama la dirección local (MAC) origen y destino. Luego, la capa de enlace de datos transmite los bits binarios de la trama a través de los medios de la capa física.

Cuando los datos se transmiten simplemente en una red de área local, se habla de las unidades de datos en términos de tramas, debido a que la dirección MAC es todo lo que se necesita para llegar desde el host origen hasta el host destino. Pero si se deben enviar los datos a otro host a través de una red interna o Internet, los paquetes se transforman en la unidad de datos a la que se hace referencia.

Esto se debe a que la dirección de red del paquete contiene la dirección destino final del host al que se envían los datos (el paquete). Las tres capas inferiores (red, enlace de datos, física) del modelo OSI son las capas principales de transporte de los datos a través de una red interna o de Internet. La excepción principal a esto es un dispositivo denominado gateway.

Este es un dispositivo que ha sido diseñado para convertir los datos desde un formato, creado por las capas de aplicación, presentación y sesión, en otro formato. De modo que el gateway utiliza las siete capas del modelo OSI para hacer esto.

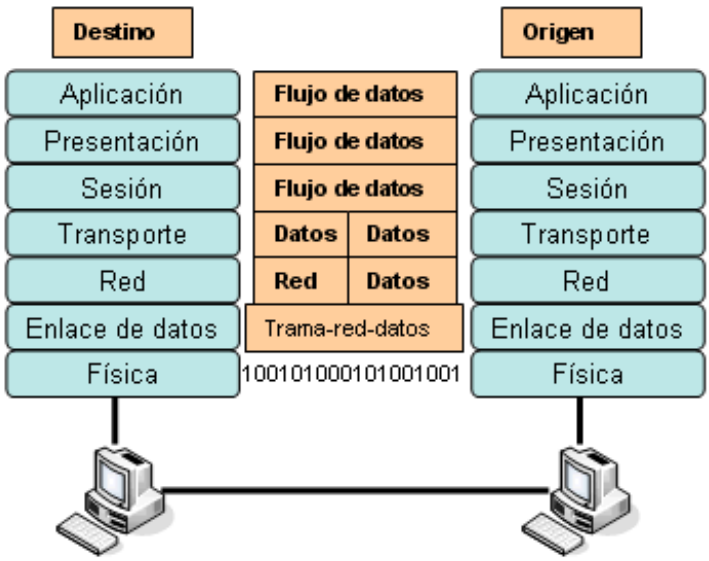


Figura 1.3 Encapsulamiento de datos

Flujo de paquetes a través de los dispositivos de Capa 2

Es importante recordar que los paquetes se ubican dentro de tramas, de modo que para comprender la forma en que viajan los paquetes en los dispositivos de la Capa 2, es necesario trabajar con la forma en que se encapsulan los paquetes, que es la trama. Cualquier cosa que le suceda a la trama también le sucede al paquete.

Las NIC, los puentes y los switches involucran el uso de la información de la dirección de enlace de datos (MAC) para dirigir las tramas. Las NIC son el lugar donde reside la dirección MAC exclusiva. La dirección MAC se utiliza para crear la trama. Los puentes examinan la dirección MAC de las tramas entrantes. Si la trama es local (con una dirección MAC en el mismo segmento de red que el puerto de entrada del puente), entonces la trama no se envía a través del puente. Si la trama no es local (con una dirección MAC que no está en el puerto de entrada del puente), entonces se envía al segmento de red siguiente. El puente toma una trama, la remueve, examina la dirección MAC y luego envía o no la trama, según lo que requiera la situación. El switch es como un hub con puertos individuales que actúan como puentes. El switch toma una trama de datos, la lee, examina las direcciones MAC de la Capa 2 y envía las tramas (las conmuta) a los puertos adecuados.

1.6 Segmentación

Con los switches se crean pequeños dominios, llamados segmentos, conectando un pequeño hub de grupo de trabajo a un puerto de switch o bien se aplica micro segmentación la cual se realiza conectando cada estación de trabajo y cada servidor directamente a puertos de switch teniendo una conexión dedicada dentro de la red.

Con lo que se consigue aumentar considerablemente el ancho de banda a disposición de cada usuario. Una de las ventajas que se pueden notar en las VLAN es la reducción en el tráfico de la red ya que solo se transmiten los paquetes a los dispositivos que estén incluidos dentro del dominio de cada VLAN, una mejor utilización del ancho de banda y confidencialidad respecto a personas ajenas a la VLAN, alta performance, reducción de latencia, facilidad para armar grupos de trabajo.

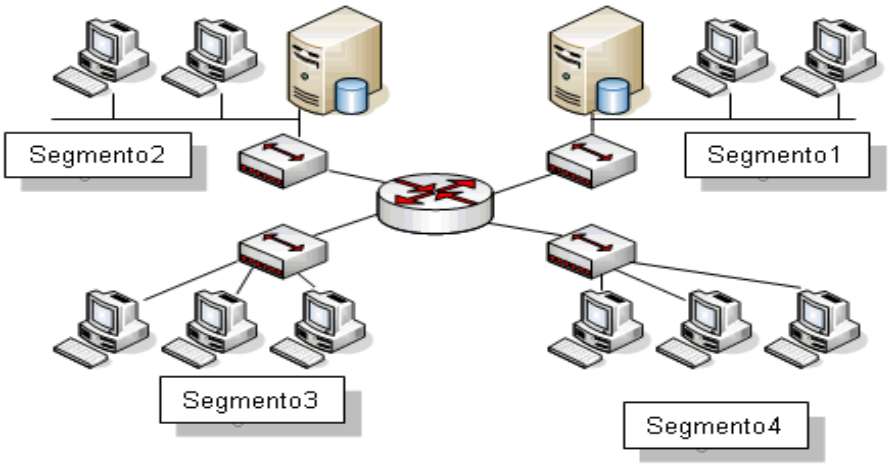


Figura 1.4 Segmentación de una red

1.7 Dominios de Colisión y Difusión

Ethernet es una tecnología conflictiva, todos los equipos de trabajo que se conectan al mismo medio físico reciben las señales enviadas por otros dispositivos.

Si dos estaciones transmiten a la vez se genera una colisión. Si no existieran mecanismos que detectaran y corrigieran los errores de estas colisiones, Ethernet no podría funcionar.

En el diseño de una red se debe tener especial cuidado con los llamados Dominios de Colisión y Dominio de difusión (Broadcast)

Dominio de colisión: Grupo de dispositivos conectados al mismo medio físico, de tal manera que si dos dispositivos acceden al medio al mismo tiempo, el resultado será una colisión entre las dos señales.

Como resultado de estas colisiones se produce un consumo inadecuado de recursos y de ancho de banda. Cuanto menor sea la cantidad de dispositivos afectados a un dominio de colisión mejor desempeño de la red.

Dominio de difusión. Grupo de dispositivos de la red que envían y reciben mensajes de difusión entre ellos. Una cantidad inapropiada de estos mensajes de difusión (broadcast) provocara un bajo rendimiento en la red, una cantidad exagerada (tormenta de broadcast) dará como resultado el mal funcionamiento de la red hasta tal punto de poder dejarla completamente congestionada.

Los hubs o concentradores tienen un único dominio de colisión, eso quiere decir que si dos equipos provocan una colisión en un segmento asociado a un puerto del hubs, todos los demás dispositivos aun estando en diferentes puertos se verán afectados. De igual manera se verían afectados si una estación envía un Broadcast, debido a que un hub también tiene un solo dominio de difusión.

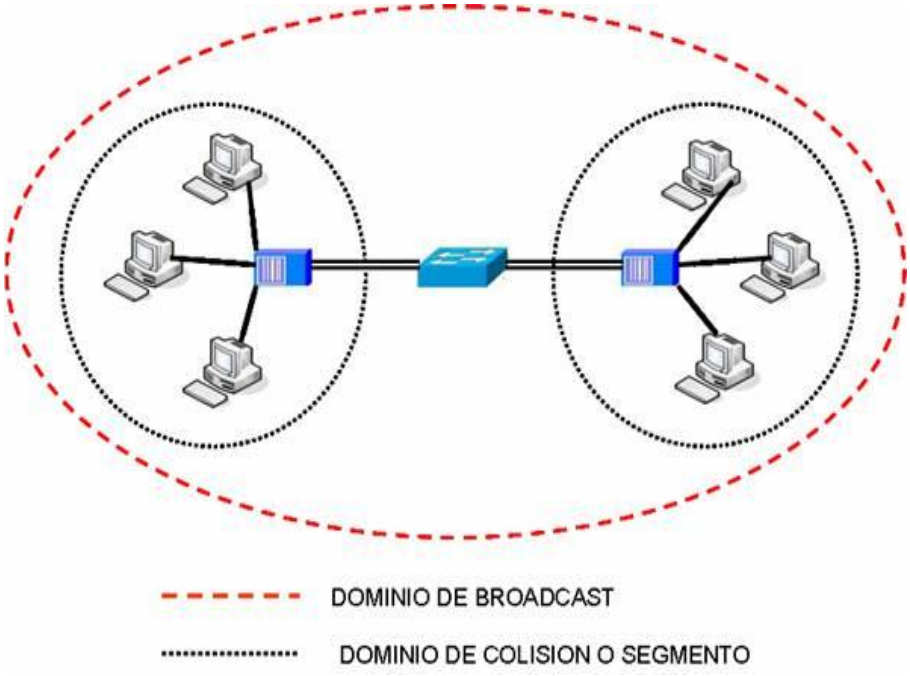


Figura 1.5 Dominios de colisión

CAPITULO 2

VIRTUAL LAN

CAPITULO 2. VIRTUAL LAN

2.1 Descripción General

Una VLAN (acrónimo de Virtual LAN) es una subred IP separada de manera lógica, las redes de área local virtuales VLAN permiten que redes IP y subredes múltiples existan en la misma red conmutada. Una característica importante de la conmutación de Ethernet es la capacidad de crear VLAN. Una VLAN es un agrupamiento lógico de estaciones y dispositivos de red. Las VLAN se pueden agrupar por funciones laborales o departamentos, sin importar la ubicación física de los usuarios.

El tráfico entre VLAN está restringido. Los switches y los puentes envían tráfico unicast, multicast y broadcast solo en segmentos de LAN que atienden a la VLAN a la que pertenece el tráfico. En otras palabras, los dispositivos en la VLAN sólo se comunican con los dispositivos que están en la misma VLAN. Los routers suministran conectividad entre diferentes VLAN. Las VLAN mejoran el desempeño general de la red agrupando a los usuarios y los recursos de forma lógica. Las VLAN pueden mejora la escalabilidad, seguridad y gestión de red.

Los routers en las topologías de VLAN proporcionan filtrado de broadcast, seguridad y gestión de flujo de tráfico.

Las VLAN que están correctamente diseñadas y configuradas son herramientas potentes para los administradores de red. Las VLAN simplifican las tareas cuando es necesario al ser agregados, mudanzas y modificaciones en una red.

Las VLAN mejoran la seguridad de la red y ayudan a controlar los broadcast de capa tres del modelo OSI. Sin embargo, cuando se les configura de manera incorrecta las VLAN pueden hacer que una red funcione de manera deficiente o que no funcione en absoluto.

La configuración e implementación correcta de las VLAN son fundamentales para el proceso de diseño de red.

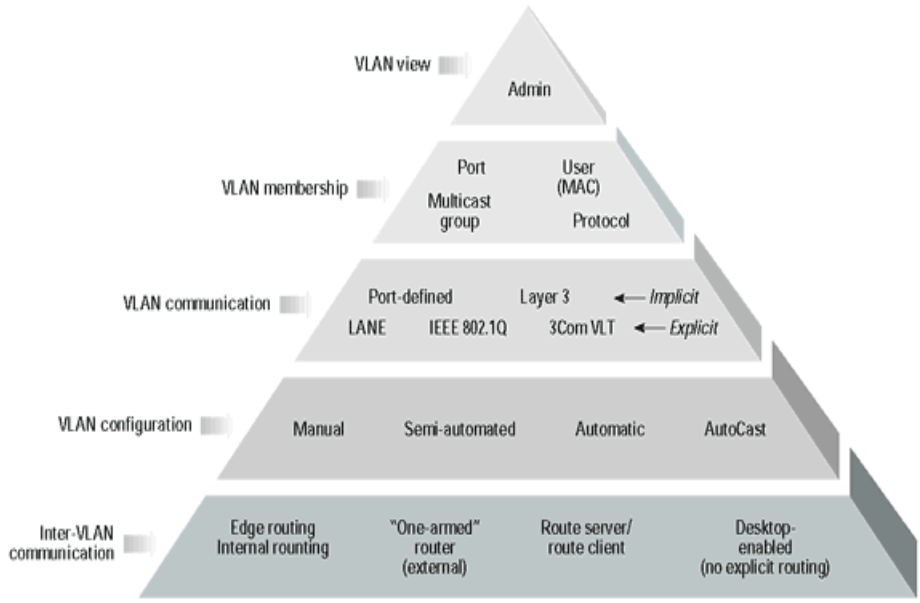


Figura 2.1 Proceso para el diseño de una red.

2.2 Clasificación 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 están en uso.

VLAN Nativa.- una VLAN nativa está asignada 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 enlace 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.

2.3 Tipos de VLAN

VLAN Estáticas

Los puertos del switch están ya pre asignados a las estaciones de trabajo

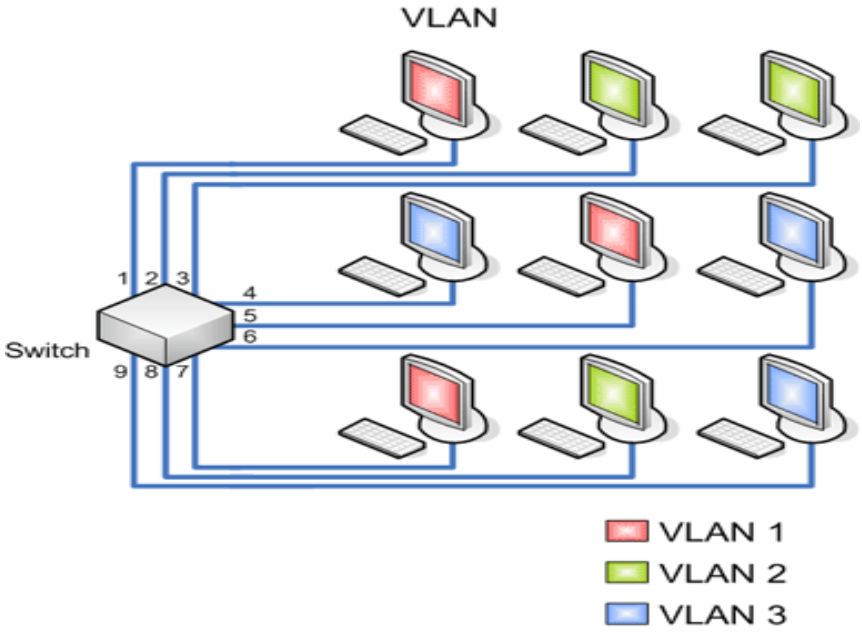


Figura 2.2 Segmento de una red por medio de VLAN's

Se han definido diversos tipos de VLAN, según criterios de conmutación y el nivel en el que se lleve a cabo:

VLAN por Puerto.- este tipo es el más sencillo ya que un grupo de puertos forma una VLAN -un puerto solo puede pertenecer a una VLAN - , el problema se presenta cuando se quieren hacer VLAN por MAC ya que la tarea es compleja. Aquí el puerto del switch pertenece a una VLAN, por tanto, si alguien posee un servidor conectado a un puerto y este pertenece a la VLAN verde, el servidor estará en la VLAN verde.

Puerto	VLAN
1	1
2	2
3	2
4	3
5	1

Tabla 2.1 Asignación de puertos de un switch a una VLAN

Ventajas:

- Facilidad de movimientos y cambios.
- Micro segmentación y reducción del dominio de Broadcast.
- Multiprotocolo: La definición de la VLAN es independiente del o los protocolos utilizados, no existen limitaciones en cuanto a los protocolos utilizados, incluso permitiendo el uso de protocolos dinámicos.

Desventajas:

- Administración: Un movimiento en las estaciones de trabajo hace necesaria la reconfiguración del puerto del switch al que está conectado el usuario. Esto se puede facilitar combinando con mecanismos de LAN Dinámicas.

VLAN por MAC.- se basa en MAC Address, por lo que se realiza un mapeo para que el usuario pertenezca a una determinada VLAN. Obviamente dependerá de la política de creación. Este tipo de VLAN ofrece mayores ventajas, pero es complejo porque hay que meterse con las direcciones MAC y si no se cuenta con un software que las administre, será muy laborioso configurar cada una de ellas.

MAC	VLAN
12.15.89.bb.1d.aa	1
aa.15.89.b2.15.aa	2
1d.15.89.6b.6d.ca	2
12.aa.cc.bb.1d.aa	3

Tabla 2.2 Mac address en una determinada Vlan.

Ventajas:

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

Desventajas:

- Problemas de rendimiento y control de Broadcast: el tráfico de paquetes de tipo Multicast y Broadcast se propagan por todas las VLAN's.
- Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo. También se puede emplear soluciones de DVLAN.

VLAN por Protocolo.- permite crear una red virtual por tipo de protocolo (por ejemplo, TCP/IP, IPX, AppleTalk, etc.). Por lo tanto, se pueden agrupar todos los equipos que utilizan el mismo protocolo en la misma red.

Las ventajas que se obtienen con este tipo de VLAN radican en que dependiendo del protocolo que use cada usuario, este se conectara automáticamente a la VLAN correspondiente.

MAC	VLAN
IP	**1**
IPX	**2**
IPX	**2**
IP	**1**

Tabla 2.3 Asignación de Ip a Vlan

Ventajas:

- Segmentación por protocolo.
- Asignación dinámica.

Desventajas

- Problemas de rendimiento y control de Broadcast: Por las búsquedas en tablas de pertenencia se pierde rendimiento en la VLAN.
- No soporta protocolos de nivel 2 ni dinámicos.

VLAN basada en la dirección de red conecta subredes según la dirección IP de origen de los datagramas. Este tipo de solución brinda gran flexibilidad, en la medida en que la configuración de los conmutadores cambia automáticamente cuando se mueve una estación. En contrapartida, puede haber una ligera disminución del rendimiento, ya que la información contenida en los paquetes debe analizarse detenidamente.

Ventajas:

- Facilidad en los cambios de estaciones de trabajo: cada estación de trabajo al tener asignada una dirección IP en forma estática no es necesario reconfigurar el switch.

Desventajas:

- El tamaño de los paquetes enviados es menor que en el caso de utilizar direcciones MAC.
- Pérdida de tiempo en la lectura de las tablas.
- Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo.

VLAN Dinámicas (DVLAN)

Las VLAN dinámicas son puertos del switch que automáticamente determinan a que VLAN pertenece cada puesto de trabajo. El funcionamiento de estas VLAN's se basa en las direcciones MAC, direcciones lógicas o protocolos utilizados. Cuando un puesto de trabajo pide autorización para conectarse a la VLAN el switch chequea la dirección MAC ingresada previamente por el administrador en la base de datos de las mismas y automáticamente se configura el puerto al cual corresponde por la configuración de la VLAN.

El mayor beneficio de las DVLAN es el menor trabajo de administración dentro del armario de comunicaciones cuando se cambian de lugar las estaciones de trabajo o se agregan y también notificación centralizada cuando un usuario desconocido pretende ingresar en la red.

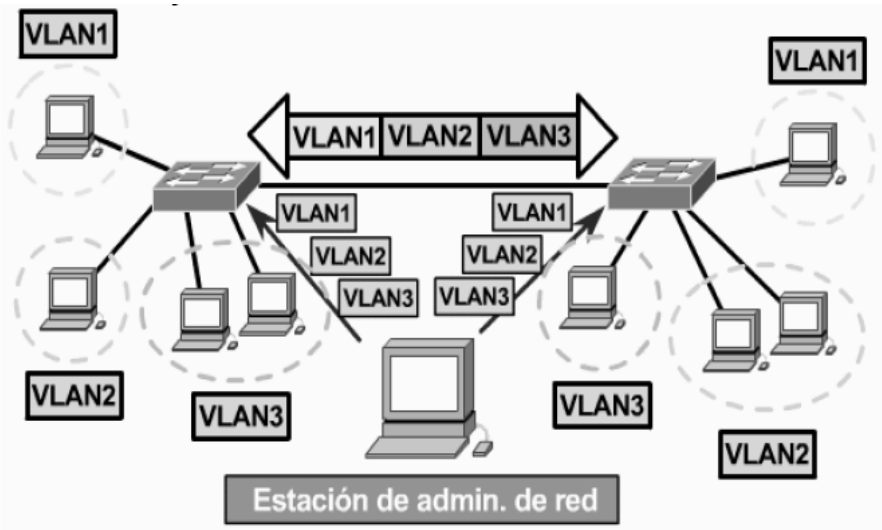


Figura 2.3 VLAN dinámicas Ventajas de una VLAN

La VLAN permite definir una nueva red por encima de la red física y, por lo tanto, ofrece las siguientes ventajas:

- Mayor flexibilidad en la administración y en los cambios de la red, ya que la arquitectura puede cambiarse usando los parámetros de los conmutadores.
- Trasladar las estaciones de trabajo en la LAN.
- Agregar fácilmente estaciones de trabajo a LAN.
- Cambiar fácilmente la configuración de la LAN.
- Aumento de la seguridad, ya que la información se encapsula en un nivel adicional y posiblemente se analiza.
- Disminución y control en la transmisión de tráfico en la red

VTP VLAN Trunking Protocol

Protocolo usado para configurar y administrar VLAN's en equipos Cisco. VTP opera en 3 modos distintos:

- Servidor
- Cliente
- Transparente

Servidor: Debe haber al menos un Servidor. Desde él se pueden crear, eliminar o modificar VLAN's.

Cliente: No se pueden crear, eliminar o modificar VLAN's.

Transparente: Desde él no se puede crear, eliminar o modificar VLAN's (que afecten a los demás switches), las VLAN's que se creen en el switch mediante CLI serán sólo locales para este switch. No procesa las actualizaciones VTP recibidas, sólo las reenvía a los switches vecinos. Para conseguir conectividad entre VLAN a través de un enlace troncal entre switches, las VLAN deben estar configuradas en cada switch. El VTP proporciona un medio sencillo de mantener una configuración de VLAN coherente a través de toda la red conmutada. VTP permite soluciones de red conmutada fácilmente escalable a otras dimensiones, reduciendo la necesidad de configuración manual de la red VTP es un protocolo de mensajería de capa 2 que mantiene la coherencia de la configuración VLAN a través de un dominio de administración común, gestionando las adiciones, supresiones y cambios de nombre de las VLAN a través de las redes. Un dominio VTP son varios switches interconectados que comparten un mismo entorno VTP. Cada switch se configura para residir en un único dominio VTP.

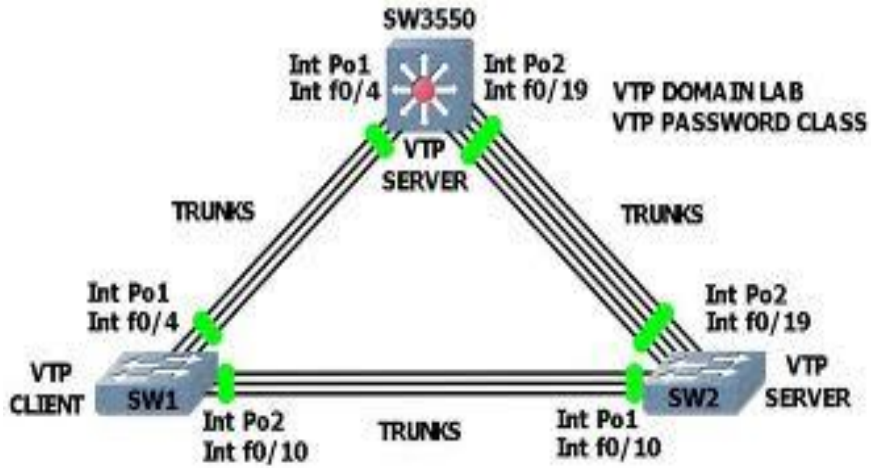


Figura 2.4 VTP en las VLAN

2.4 Enlace Troncal

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

Existen diferentes 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.

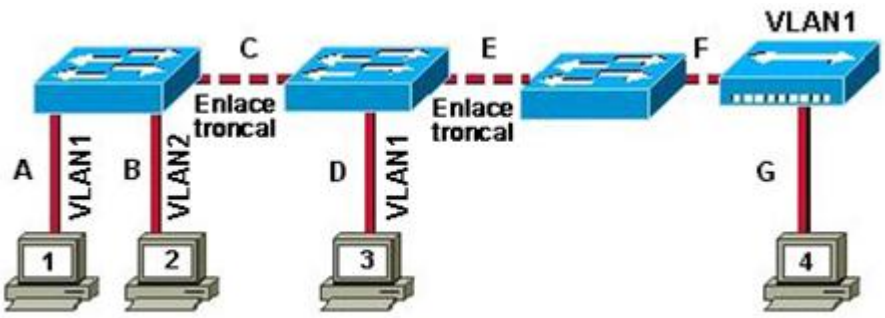


Figura 2.5 Enlace troncal

2.5 Estándares de las VLAN

El protocolo IEEE 802.1Q, también conocido como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (*Trunking*). Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet.

Formato de la trama

802.1Q en realidad no encapsula la trama original sino que añade 4 bytes al encabezado Ethernet original. El valor del campo EtherType se cambia a 0x8100 para señalar el cambio en el formato de la trama.

VLAN nativas

El punto 9 del estándar define el protocolo de encapsulamiento usado para multiplexar varias VLAN a través de un solo enlace, e introduce el concepto de las VLAN nativas. Las tramas pertenecientes a la VLAN nativa no se etiquetan con el ID de VLAN cuando se envían por el trunk.

Y en el otro lado, si a un puerto llega una trama sin etiquetar, la trama se considera perteneciente a la VLAN nativa de ese puerto.

Este modo de funcionamiento fue implementado para asegurar la interoperabilidad con antiguos dispositivos que no entendían 802.1Q.

La VLAN nativa es la vlan a la que pertenecía un puerto en un switch antes de ser configurado como trunk. Sólo se puede tener una VLAN nativa por puerto. Para establecer un trunking 802.1Q a ambos lados debemos tener la misma VLAN nativa porque la encapsulación todavía no se ha establecido y los dos switches deben hablar sobre un link sin encapsulación (usan la native VLAN) para ponerse de acuerdo en estos parámetros. En los equipos de Cisco Systems la VLAN nativa por defecto es la VLAN 1

Durante el diseño se recomienda

- La VLAN nativa no debe ser la de gestión.
- Cambiar la VLAN nativa de la 1 a cualquier otra como medida de seguridad.
- Todos los switches en la misma VLAN nativa.
- Usuarios y servidores en sus respectivas VLAN’s.

- El tráfico entre switches debe ser el único que no se encapsule en enlaces trunk. El resto del tráfico, incluyendo la VLAN de gestión debe ir encapsulado por los trunks. Si no estamos encapsulando cualquiera puede conectar un equipo que no hable 802.1q (switches y hubs) y funcionará sin nuestro control.

2.6 Beneficios de implementar una VLAN

La principal excusa para implementar una VLAN es la reducción en el costo de los cambios y movimientos de usuarios. Desde que estos costos son bastante sustanciales, este argumento es suficientemente obligatorio para la implementación de una VLAN.

Muchos fabricantes están prometiendo que la implementación de una VLAN resultará más conveniente a la hora de habilitar la administración de redes dinámicas, y que esto supondrá bastante ahorro. Esta promesa se puede aplicar con buenos resultados a redes IP, ya que, normalmente, cuando un usuario se mueve a una diferente subred, las direcciones IP han de ser actualizadas manualmente en la estación de trabajo. Este proceso consume gran cantidad de tiempo que podría ser aprovechado para otras tareas, tales como producir nuevos servicios de red.

Una VLAN elimina ese hecho, porque los miembros de una red virtual no están atados a una localización física en la red, permitiendo que las estaciones cambiadas de sitio conserven su dirección IP original.

Sin embargo, cualquier implementación de VLAN no reduce este costo. Una VLAN añade una nueva capa de conexión virtual que ha de ser administrada al mismo tiempo que la conexión física. Esto no quiere decir que no se puedan reducir los costes hablados anteriormente.

2.7 Enrutamiento entre VLAN

El enrutamiento entre VLAN’s o inter VLAN routing, resulta necesario una vez que se posee una infraestructura de red con VLAN implementadas, debido a que los usuarios necesitaran intercambiar información de una red a otra.

Es importante recordar que cada VLAN es un dominio de broadcast único. Por lo tanto, de manera predeterminada, las computadoras en VLAN separadas no pueden comunicarse.

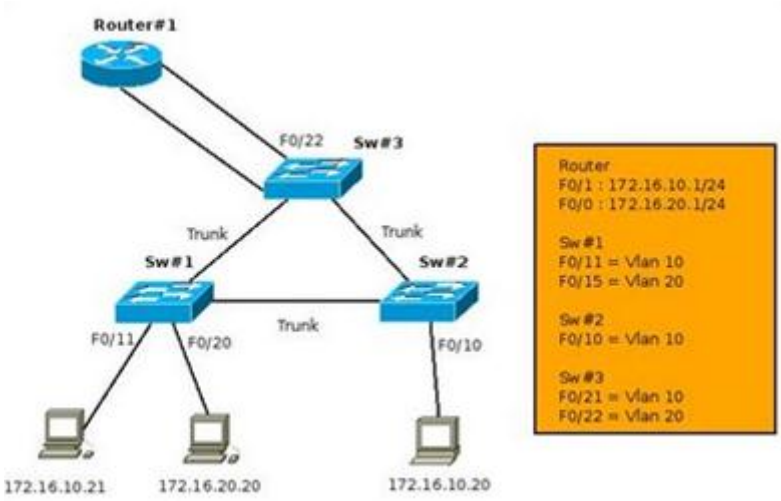


Figura 2.6 Enrutamiento de una VLAN

Existe una manera para permitir que estas estaciones finales puedan comunicarse; esta manera se llama enrutamiento entre vlan (Inter vlan routing).

El enrutamiento entre VLAN es un proceso que permite reenviar el tráfico de la red desde una VLAN a otra mediante un enrutador. Las VLAN están asociadas a subredes IP únicas en la red.

Esta configuración de subred facilita el proceso de enrutamiento en un entorno de múltiples VLAN.

Tradicionalmente, el enrutamiento de la LAN utiliza enrutadores con interfaces físicas múltiples.

Es necesario conectar cada interfaz a una red separada y configurarla para una subred diferente.

En una red tradicional que utiliza múltiples VLAN para segmentar el tráfico de la red en dominios de broadcast lógicos, el enrutamiento se realiza mediante la conexión de diferentes interfaces físicas del enrutador a diferentes puertos físicos del switch.

Los puertos del switch conectan al enrutador en modo de acceso; en este modo, diferentes VLAN estáticas se asignan a cada interfaz del puerto.

Cada interfaz del switch estaría asignada a una VLAN estática diferente. Cada interfaz del enrutador puede entonces aceptar el tráfico desde la VLAN asociada a la interfaz del switch que se encuentra conectada y el tráfico puede enrutarse a otras VLAN conectadas a otras interfaces. El enrutamiento entre VLAN tradicional requiere de interfaces físicas múltiples en el enrutador y en el switch. Sin embargo, no todas las configuraciones del enrutamiento entre VLAN requieren de interfaces físicas múltiples. Algunos software del enrutador permiten configurar interfaces del enrutador como enlaces troncales. Esto abre nuevas posibilidades para el enrutamiento entre VLAN. "enrutador-on-a-stick" es un tipo de configuración de enrutador en la cual una interfaz física única enruta el tráfico entre múltiples VLAN en una red.

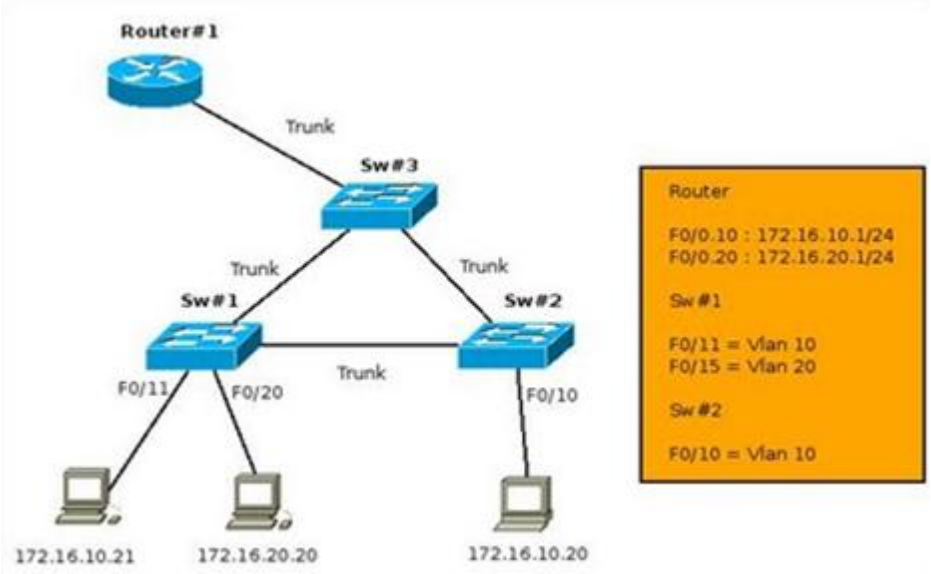


Figura 2.7 Enrutamiento entre VLAN (Subinterfaces)

La interfaz del enrutador se configura para funcionar como enlace troncal y está conectada a un puerto del switch configurado en modo de enlace troncal. El enrutador realiza el enrutamiento entre VLAN al aceptar el tráfico etiquetado de la VLAN en la interfaz troncal proveniente del switch adyacente y enrutar en forma interna entre las VLAN, mediante subinterfaces.

El enrutador luego reenvía el tráfico enrutado de la VLAN etiquetada para la VLAN de destino por la misma interfaz física.

Las subinterfaces son interfaces virtuales múltiples, asociadas a una interfaz física. Estas interfaces están configuradas en software en un enrutador configurado en forma independiente con una dirección IP y una asignación de VLAN para funcionar en una VLAN específica. Las subinterfaces están configuradas para diferentes subredes que corresponden a la asignación de la VLAN, para facilitar el enrutamiento lógico antes de que la VLAN etiquete las tramas de datos y las reenvíe por la interfaz física. Aprenderá más acerca de las interfaces y las subinterfaces en el siguiente tema.

2.8 Interfaces y subinterfaces

El enrutamiento tradicional requiere de enrutadores que tengan interfaces físicas múltiples para facilitar el enrutamiento entre VLAN. El enrutador realiza el enrutamiento al conectar cada una de sus interfaces físicas a una VLAN única. Además, cada interfaz está configurada con una dirección IP para la subred asociada con la VLAN conectada a ésta.

Al configurar las direcciones IP en las interfaces físicas, los dispositivos de red conectados a cada una de las VLAN pueden comunicarse con el enrutador mediante la interfaz física conectada a la misma VLAN. En esta configuración los dispositivos de red pueden utilizar el enrutador como un gateway para acceder a los dispositivos conectados a las otras VLAN.

CAPITULO 3

SUBNETEO

CAPITULO 3. SUBNETEO

La función del Subneteo o Subnetting es dividir una red IP física en subredes lógicas (redes más pequeñas) para que cada una de esta trabajen a nivel envío y recepción de paquetes como una red individual, aunque todas pertenezcan a la misma red física y al mismo dominio.

El Subneteo permite una mejor administración, control del tráfico y seguridad al segmentar la red por función. También, mejora la performance de la red al reducir el tráfico de broadcast de nuestra red. Como desventaja, su implementación desperdicia muchas direcciones, sobre todo en los enlaces seriales.

Dirección IP

Las direcciones IP están compuestas por 32 bits divididos en 4 octetos de 8 bits cada uno. A su vez, un bit o una secuencia de bits determinan la Clase a la que pertenece esa dirección IP.

Cada clase de una dirección de red determina una máscara por defecto, un rango IP, cantidad de redes y de hosts por red. Cada Clase tiene una máscara de red por defecto, la Clase A 255.0.0.0, la Clase B 255.255.0.0 y la Clase C 255.255.255.0. Al direccionamiento que utiliza la máscara de red por defecto, se lo denomina “direccionamiento con clase” (classful addressing).

Siempre que se subnetea se hace a partir de una dirección de red Clase A, B, o C y está se adapta según los requerimientos de subredes y hosts por subred. Tengan en cuenta que no se puede subnetear una dirección de red sin Clase ya que ésta ya pasó por ese proceso, aclaro esto porque es un error muy común.

Al direccionamiento que utiliza la máscara de red adaptada (subneteada), se lo denomina “direccionamiento sin clase”. En consecuencia, la Clase de una dirección IP es definida por su máscara de red y no por su dirección IP. Si una dirección tiene su máscara por defecto pertenece a una Clase A, B o C, de lo contrario no tiene Clase aunque por su IP pareciese la tuviese.

Máscara de Red

La máscara de red se divide en 2 partes:

3.1 Porción de Red

En el caso que la máscara sea por defecto, una dirección con Clase, la cantidad de bits “1” en la porción de red, indican la dirección de red, es decir, la parte de la dirección IP que va a ser común a todos los hosts de esa red. En el caso que sea una máscara adaptada, el tema es más complejo.

La parte de la máscara de red cuyos octetos sean todos bits “1” indican la dirección de red y va a ser la parte de la dirección IP que va a ser común a todos los hosts de esa red, los bits “1” restantes son los que en la dirección IP se van a modificar para generar las diferentes subredes y van a ser común solo a los hosts que pertenecen a esa subred.

En ambos casos, con Clase o sin, se determina el prefijo que se suele ver después de una dirección IP (ej: /8, /16, /24, /18, etc.) ya que ese número es la suma de la cantidad de bits “1” de la porción de red.

3.2 Porción de Host

La cantidad de bits "0" en la porción de host de la máscara, indican que parte de la dirección de red se usa para asignar direcciones de host, es decir, la parte de la dirección IP que va a variar según se vayan asignando direcciones a los hosts.

Si tenemos la dirección IP Clase C 132.18.0.0/22 (red subneteada), en los 2 primeros octetos de la dirección IP, ya que los 2 primeros octetos de la máscara de red tienen todos bits “1” (fondo bordo), es la dirección de red y va a ser común a todas las subredes y hosts. Como el 3º octeto está divido en 2, una parte en la porción de red y otra en la de host, la parte de la dirección IP que corresponde a la porción de red (fondo negro), que tienen en la máscara de red los bits “1”, se va a ir modificando según se vayan asignando las subredes y solo va a ser común a los host que son parte de esa subred. Los 2 bits “0” del 3º octeto en la porción de host (fondo gris) y todo el último octeto de la dirección IP, van a ser utilizados para asignar direcciones de host.

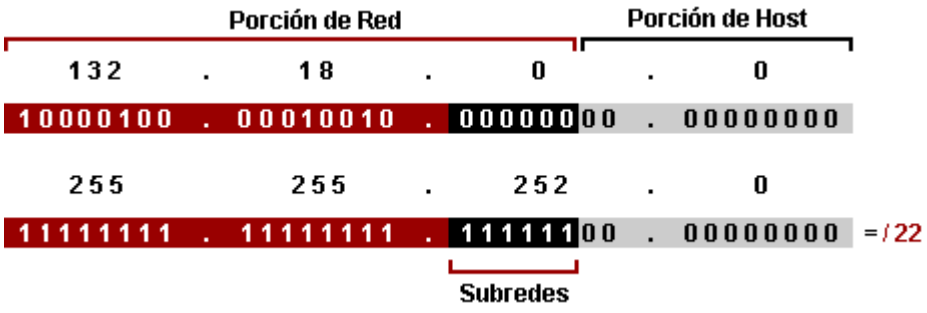


Figura 3.1 Calculo de direcciones host

Convertir Bits en Números Decimales

Como sería casi imposible trabajar con direcciones de 32 bits, es necesario convertirlas en números decimales. En el proceso de conversión cada bit de un intervalo (8 bits) de una dirección IP, en caso de ser "1" tiene un valor de "2" elevado a la posición que ocupa ese bit en el octeto y luego se suman los resultados.

Posición y Valor de los Bits									
	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Binario	1	0	0	0	0	0	0	0	= 128
Decimal	128	0	0	0	0	0	0	0	+
Binario	0	1	0	0	0	0	0	0	= 64
Decimal	0	64	0	0	0	0	0	0	+
Binario	0	0	1	0	0	0	0	0	= 32
Decimal	0	0	32	0	0	0	0	0	+
Binario	0	0	0	1	0	0	0	0	= 16
Decimal	0	0	0	16	0	0	0	0	+
Binario	0	0	0	0	1	0	0	0	= 8
Decimal	0	0	0	0	8	0	0	0	+
Binario	0	0	0	0	0	1	0	0	= 4
Decimal	0	0	0	0	0	4	0	0	+
Binario	0	0	0	0	0	0	1	0	= 2
Decimal	0	0	0	0	0	0	2	0	+
Binario	0	0	0	0	0	0	0	1	= 1
Decimal	0	0	0	0	0	0	0	1	= 255

Figura 3.2 Tabla de conversiones en números decimales

La combinación de 8 bits permite un total de 256 combinaciones posibles que cubre todo el rango de numeración decimal desde el 0 (00000000) hasta el 255 (11111111).

Calcular la Cantidad de Subredes y Hosts por Subred

Cantidad de Subredes es igual a: 2N, donde "N" es el número de bits "tomados" de la porción de Host.

Cantidad de Hosts x Subred es igual a: 2M -2, donde "M" es el número de bits disponible en la porción de host y "-2" es debido a que toda subred debe tener su propia dirección de red y su propia dirección de broadcast.

CAPITULO 4

IMPLEMENTACIÓN DE GRUPOS DE TRABAJO POR MEDIO DE VLAN

CAPITULO 4. IMPLEMENTACIÓN DE GRUPOS DE TRABAJO POR MEDIO DE VLAN

4.1 Estado Actual

El estado actual de la red en el 5to y 6to piso del edificio es la siguiente:

En el 5to piso se encuentran 8 switches de 24 puertos cada uno, en estos switches de encuentran los siguientes departamentos:

- Dirección General.
- Finanzas.
- Recursos Materiales y Servicios.
- Recursos Humanos.

En estos departamentos se encuentran conectados 180 usuarios a los switches sin ningún tipo de organización.

4.2 Pruebas de comunicación antes de configuración

Antes de hacer todo el planteamiento se hicieron pruebas de conectividad entre varias PC, esto con el fin de verificar que todas las PC tuvieran conectividad y de esta manera ver la importancia de la segmentación de redes.

Se procedió a realizar una prueba de comunicación entre dos PC's de diferentes departamentos, donde observamos que al momento de hacer el llamado de una PC a otra responde sin ningún problema.

Para mayor referencia consultar Anexo 1 Comunicación antes de la configuración.

En el 6to. Piso se encuentras 6 switches de 24 puertos. Cada uno.
Los departamentos que se encuentran en este piso, son las siguientes:

- Coordinación Administrativa
- Soporte técnico
- Intendencia

Con 120 usuarios en este piso, los cuales se encuentran conectados a estos switches.

4.3 Cálculo de Máscara para la subred

Ésta es la red que actualmente se tiene en sitio y a la cual se le realizará el proceso de subneteo que actualmente no tiene y que presenta conflictos de tráfico. Red 192.168.1.0 /24 Para realizar éste cálculo nos basamos en el número actual de equipos disponibles por departamento. 30 Host por subred.

Teniendo éste valor podemos calcular de acuerdo al último octeto de la máscara de red cuantos bits son necesarios para contener a todos los host. Realizamos el cálculo basados en la siguiente fórmula:

$2^N – 2$ = Número de hosts

Utilizando la formula anterior:

$2^5 – 2 = 30$ host

Utilizando 3 bit para definir la máscara de las subredes, quedando como sigue: Máscara de 27 bits.

11111111	**.**	**11111111**	**.**	**11111111**	**.**	**11100000**
255	.	255	.	255	.	224

Tabla 4.1 Cálculo para mascara de subred

4.4 Asignación de puerto a la VLAN

Como podemos observar, N es el número de bits que se toman del último octeto de la máscara y son colocados a 0 para definir que serán ocupados por host y no son parte de la subred.

PUERTO	VLAN	SWITCH
1,2,21	Directivos	Piso 6
15,16,22	Finanzas	Piso 6
3,7,11	Materiales	Piso 5
14,8,10	Soporte	Piso 5
23,17,19	Intendencia	Piso 5
4,5,18	Procesos	Piso 6

Tabla 4.2 Asignación de puerto a una Vlan

Se revisaron los equipos disponibles en sitio y se generó la configuración que se presenta en la tabla anterior para asignar los segmentos de red a cada departamento.

4.5 Direccionamiento IP de VLAN's

Al tener definidos los puertos que se van a utilizar en cada switch para un departamento, podemos hacer la asignación de la VLAN correspondiente al departamento deseado independientemente del piso en el cuál se encuentra ubicado el equipo (host). Como se muestra en la siguiente tabla:

Dirección IP	VLAN	No. VLAN
192.168.1.0 /27	Vlan Procesos	6
192.168.1.32 / 27	Vlan Finanzas	3
192.168.1.64 / 27	Vlan Materiales	4
192.168.1. 96 / 27	Vlan Soporte	5
192.168.1.128 / 27	Vlan Intendencia	7
192.168.1.160 / 27	Vlan Directivos	2

Tabla 4.3 Asignación de IP´s a Departamentos.

Ahora para que la transmisión de datos se realice correctamente los equipos (host) también deben de tener asignada una IP fija, ya que con ésta serán reconocidas dentro de la subred y tendrán acceso a los recursos disponibles.

Por defecto los host tienen configurada la opción de generar una IP automáticamente dependiendo de un algoritmo propio del sistema operativo, esto nos puede traer problemas al momento de crear dicha IP, ya que si no corresponde al segmento de red definido en el switch, simplemente no se podría comunicar en la subred.

Por lo tanto realizamos la asignación manual de la IP para asegurar que el segmento de red sea el correcto y el equipo sea reconocido correctamente por el switch al cuál se encuentre conectado y por el cual se realiza la transmisión de los datos.

También es importante definir el tipo de máscara que utiliza el host, ya que en caso de ser una diferente a la que se tiene configurada no será reconocido en el segmento de red al cual está conectado en el switch, y por lo tanto no habría comunicación y los paquetes enviados estarían viajando únicamente en el cable de red que conecta el equipo con el switch.

4.6 Asignación de IP a equipos de trabajo (PC)

Una vez que se tiene configurados los switches, procedemos a configurar todos y cada uno de los equipos de trabajo, tomando en cuenta que cada equipo tiene que ir con la configuración de IP correspondiente a la VLAN que le corresponda.

Para asignar la IP a cada equipo procedemos a entrar a las configuraciones de la red, posteriormente asignaremos la IP correspondiente a la VLAN en la que se desea agregar dicha PC, para mayor referencia de rangos de VLAN ver Tabla 2.3.

Es importante definir que no podemos usar ni la primera IP ni la última, debido a que la primera IP de cada una de nuestras VLAN define el segmento de red y la última define nuestro broadcast.

En la siguiente imagen veremos un ejemplo de cómo tenemos que definir la IP al equipo, en este caso declararemos la IP de una PC que será parte de la VLAN de Finanzas, como no podemos tomar la primera IP ni la ultima, procedemos a tomar la primera IP de nuestra VLAN más uno.

Para las PC's consecutivas vamos a tomar una IP que no haya sido utilizada anteriormente por alguna otra PC, de modo que no se tengan IP's repetidas.

Para mayor referencia consultar Anexo 2 Asignación de IP a equipo de trabajo (PC)

En caso que se desee cambiar la pertenencia a la VLAN, de igual manera se deberá cambiar la IP de la PC, está deberá corresponder a alguna IP que no se encuentre ocupada en la VLAN en la que se desea pertenecer.

4.7 Configuración de enlace troncal

Para iniciar la configuración de los equipos de interconexión vamos a empezar a configurar los enlaces troncales, primeramente identificamos los puertos por los que se estén conectados los switches, teniendo los puertos previamente identificados procedemos a configurar los puertos para hacer esto nos ayudamos del siguiente comando:

```
PISO6>enable
PISO6#configure terminal
PISO6(config)#interface Interface-id
PISO6(config-if)#switchport mode trunk
```

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.

Para mayor referencia consultar Anexo 3 Configuración de enlace troncal.

Este paso se beberá repetir hasta tener todos y cada uno de los switches configurados con su respectivo enlace troncal.

Una vez configurado los enlaces verificamos que la interfaz configurada tenga los cambios aplicados, esto lo hacemos con el siguiente comando:

 # show running-config

Este comando muestra la configuración del switch.

Para mayor referencia consultar Anexo 4 Utilidad del comando show running-config

4.8 Configuración de VTP

Una vez que los enlaces troncales estén configurados, procedemos a configurar los switch con los VTP. Para esto es necesario configurar un switch en modo servidor y todos los demás deberán ir en modo cliente, con el fin de que solamente uno sea el encargado de decirle a los demás las altas y bajas de las VLAN. Los administradores cambian la configuración de las VLANs en el switch 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.

4.9 Configuración del VTP Server

Para configurar el switch en modo servidor debemos de seguir los siguientes comandos:

```
PISO6>enable
PISO6#configure terminal
PISO6(config)#vlan database
PISO6(vlan)#vtp tipo-vtp
PISO6(vlan)#vtp domain nombre-dominio
```

Donde:

- vlan database.- Comando para entrar al modo de configuración de vtp.
- vtp tipo-vtp.- Define el tipo de VTP (server).
- vtp domain nombre-dominio.- Nombre del dominio a utilizar en el VTP, deberá utilizarse el mismo en modo servidor y cliente.

Para mayor referencia consultar Anexo 5 Configuración VTP en modo SERVIDOR.

Recordemos que únicamente uno de nuestros switch va a estar en modo servidor ya que este es el que va a estar encargado de replicar las VLAN que demos de alta en él.

4.10 Configuración del VTP Cliente

Para configurar el switch en modo cliente debemos de seguir los siguientes comandos:

```
PISO6>enable
PISO6#configure terminal
PISO6(config)#vlan database
PISO6(vlan)#vtp tipo-vtp
PISO6(vlan)#vtp domain nombre-dominio
```

Donde:

- vlan database.- Comando para entrar al modo de configuración de vtp.
- vtp tipo-vtp.- Define el tipo de VTP (client).
- vtp domain nombre-dominio.- Nombre del dominio a utilizar en el VTP, deberá utilizarse el mismo en modo servidor y cliente.

Verificamos la configuración que se realizó en el switch llamado PISO5, este es el que configuramos como cliente.

Para mayor referencia consultar Anexo 6 Configuración de VTP en modo CLIENTE.

Se debe seguir la configuración de los demás switches en modo cliente, ya que los cambios que nosotros realicemos en el switch que se encuentra en modo server se aplicaran de una manera automática en los switches que se encuentren en modo cliente.

Es importante mencionar que antes de declarar las VLAN en el switch servidor, debemos de asegurarnos de que todos los switches estén ya configurados en modo cliente para que se pueda replicar la VLAN en todos y cada uno de ellos.

Una vez realizada ambas configuraciones, tanto servidor como cliente, procedemos a verificar el estatus de cada uno de ellos para asegurarnos de que la configuración esté correcta, para ello nos vamos a auxiliar del siguiente comando:

```
# show vtp status
```

Comando para verificar el estatus de las VTP en los switches.

Primeramente verificamos el estatus del switch en modo servidor.

Para mayor referencia consultar Anexo 7 Estado de switch en modo SERVER.

Posteriormente verificamos el estado del switch que configuramos en modo cliente.

Para mayor referencia consultar Anexo 8 Estado de switch en modo CLIENTE.

4.11 Creación de VLAN

Para la creación y configuración de VLAN's el switch es necesario que se haga en el switch que se configuro como servidor en el VTP, ya que es el único donde se podrán crear o eliminar las VLAN que se creen.

Una vez entendido esto procedemos a crear las VLAN necesarias en el switch, posteriormente le asignamos el nombre para distinguir a qué grupo de trabajo pertenecen.

Para crear y nombrar una VLAN usamos el siguiente comando:

```
PISO6>enable
PISO6#configure terminal
PISO6(config)#vlan vlan-id
PISO6(config-vlan)#name nombre-vlan
```

Donde:

- vlan-id.- Número de vlan que se desea crear por ejemplo 1
- nombre-vlan.- Nombre de la VLAN que se acaba de crear, por ejemplo MIVLAN.

Para mayor referencia consultar Anexo 9 Creación y nombramiento de una VLAN.

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.

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.

Para verificar que las VLAN se crearon correctamente y que se haya cambiado correctamente el nombre corremos el siguiente comando:

show vlan

Este comando se encarga de mostrar la vlan´s configuradas

Para mayor referencia consultar Anexo 10 Utilidad del comando show vlan.

Para verificar que esté funcionando el VTP y que haya replicado las VLAN creadas anteriormente vamos a verificar el estado de las VLAN en los swicthes cliente, para aseguramos de que se haya creado todas y cada una de las VLAN’s.

Para mayor referencia consultar Anexo 11 Visualización de VLAN en switches clientes

4.12 Asignación de puertos a las VLAN

Una vez que ya se tiene toda la configuración anterior procedemos a asignar los puertos del switch a los que están conectados los equipos de trabajo.

Se deberá tener la relación de puerto – equipo de trabajo a la mano, con el fin de hacer más sencilla la configuración en el equipo, para esta configuración es necesario que se haga en todos y cada uno de los switches.

Para asignar el puerto a la VLAN usamos el siguiente comando:

```
PISO6>enable
PISO6#configure terminal
PISO6(config)# interface Interface-id
PISO6(config-if)#switchport access vlan vlan-id
```

Donde:

- Interface-id.- Tipo de puerto a configurar por ejemplo fastethernet 0/0
- vlan-id.- Número de vlan a la que se desea asignar la interface.

Para mayor referencia consultar Anexo 12 Asignación de puertos a VLAN.

Es necesario repetir este paso para todos y cada uno de los puertos donde necesitemos asignar una VLAN.

4.13 Configuración de inter VLAN's

Una vez que se tienen las configuraciones de las VLAN podemos darnos cuenta que solo va a existir la comunicación entre los Host de la misma VLAN.

Debido a que existe la necesidad de hacer la comunicación con otras áreas, necesitamos hacer una configuración inter VLAN, para que sin importar a que VLAN pertenezca exista comunicación entre las áreas.

Para poder realizarla configuración es necesario acceder al Router y configurar las VLAN que requieren comunicarse entre ellas, esto se logra con los siguientes comandos:

```
Router>enable
Router#configure  terminal
Router(config)#interface  Interface-id
Router(config-subif)#encapsulation dot1Q vlan-id
Router(config-subif)#ip address Ip-addressMask-address
```

Donde:

- Interface-id.- Tipo de puerto a configurar por ejemplo fastethernet 0/0, para las interfaces lógicas deberemos asignar un punto segido de un número que se le desea dar, por ejemplo fastethernet 0/0.1

- vlan-id.- Número de vlan a la que se desea asignar la interface.
- Ip-address.- Número de IP que se le desea asignar a la interfaz, en este caso se deberá poner una IP que se encuentre libre de la vlan a la que se desea incorporar.
- Mask-address.- Máscara de red de la que se agregó la IP.

Repetir este caso para cada una de las VLAN creadas anteriormente para asegurar la comunicación entre todas las VLAN.

Para mayor referencia consultar Anexo 13 Visualización de configuración de inter VLAN en router.

4.14 Red segmentada

Todos los departamentos quedaron en diferentes segmentos, para evitar la pérdida de recursos del ancho de banda, así el funcionamiento general de la red, será mejor al evitar el tráfico innecesario.

Como se puede ver en el **Anexo 14 Red Segmentada**, se observa que no la distribución física de las PC's del mismo grupo de trabajo no importa, ya que la configuración que se realizo fue en los dispositivos de comunicación, debido a que la implementación fue lógica, y no implico mover los equipos de su lugar de origen.

Se puede observar de igual manera una pequeña parte del como quedo segmenta la red, de donde se pueden observar los grupos de trabajos y a que VLAN pertenece cada uno de ellos.

Otra parte importante de la segmentación fue reducir los dominios de colisión que se venían generando anteriormente

4.15 Pruebas de comunicación después de configuración

Después de hacer la configuración desarrollada en el capítulo 4, hacemos las pruebas de comunicación entre PC del la misma VLAN para verificar que siga habiendo comunicación entre PC's.

En la siguiente figura podemos observar que hay una comunicación entre PC's de la misma VLAN.

Para mayor referencia consultar Anexo 15 Red Segmentada.

Posteriormente tratamos de comunicar dos PC's de diferentes VLAN, para poder ver el resultado de la configuración antes hecha, dando como

resultado la incomunicación de esta, ya que al no estar en la misma VLAN no existe comunicación.

Para mayor referencia consultar Anexo 16 Comunicación negada a PC de Finanzas a PC de Directivos.

Para poder asegurarnos que la comunicación realmente sea efectiva vamos a tratar de comunicar dos PC de diferentes departamentos una vez más para cerciorarnos de que no exista la comunicación innecesaria a departamentos. En el **Anexo 17 (Comunicación entre VLAN's Soporte-Materiales)** veremos cómo se niega la comunicación de la VLAN de SOPORTE cuando quiere acceder a la VLAN de MATERIALES.

Ahora vamos a hacer el mismo procedimiento de comunicación, pero ahora vamos hacer la prueba de comunicación entre dos PC de la VLAN SOPORTE.

Para mayor referencia consultar el Anexo 18 Comunicación entre VLAN Soporte.

Para probar la configuración de las inter VLAN vamos a tratar de hacer comunicación entre dos VLAN diferentes, una de ella será la VLAN de FINANZAS y a la cual vamos probar llegar será la VLAN de MATERIALES.

Para mayor referencia consultar Anexo 19 Comunicación entre VLAN Finanzas – Materiales.

Es importante tomar en cuenta que para poder restringir el acceso de las PC's de cualquier VLAN se deberá configurar el Router de tal manera que desde ahí por medio de ACL o Listas de Acceso, se nieguen los servicios según sea el caso, el motivo de este trabajo no está enfocado a la restricción de información, sino a la segmentación de tal manera que se agilice la red.

CONCLUSIONES

Debido a que la tecnología actual ha tenido un crecimiento acelerado, ha sido necesario implementar formas de comunicación entre los diferentes dispositivos que se pueden encontrar en una oficina. Cuando se conectan dos o más computadoras o dispositivos que contienen un identificador propio (MAC Address ó Dirección IP) se establece que los elementos se encuentran conectados en una red de área local (LAN), cuando es necesario conectar dos o más redes LAN ésta se convierte en una red de área extensa (WAN).

Al utilizar redes WAN se requiere un control en el flujo de la información, lo cual se va logrando con equipos como el Bridge y el Router, permitiendo la interconexión entre redes, de la misma y diferente clase respectivamente. Adicionalmente se utilizan diferentes procedimientos lógicos para realizar la comunicación, como encapsulamientos o tramas y dispositivos capaces de interpretar la información contenida en la trama y enviarla al destino.

Para poder tener un mejor tráfico de las tramas en la red es necesario realizar una segmentación de las redes para hacer que la red sea más eficiente. Al realizar la segmentación de la red es recomendable utilizar el subneteo para identificarla por función y mejorar su desempeño. Cuando se realiza el subneteo se crea la máscara de subred que se obtiene de la cantidad de host requeridos en cada subred.

La segmentación se puede realizar de diferentes maneras, pero la que encontramos más interesante por su capacidad de adaptarse al crecimiento y cambios dentro de la red es la creación de VLAN. Al crear una VLAN se hace un agrupamiento lógico de estaciones y dispositivos que estarán en constante comunicación. Al tener una administración virtual de una LAN se tiene la flexibilidad de agregar, eliminar o cambiar los dispositivos conectados de ubicación sin que sea necesario realizar configuraciones físicas adicionales a las del dispositivo modificado. Se eligió utilizar una VLAN por puerto para facilitar la administración, realizando cambios y movimientos de un puerto más fácilmente. Además de poder realizar una micro segmentación y reducir el dominio del Broadcast. Y por último es independiente del protocolo utilizado, por lo que permite el uso de protocolos dinámicos. Una de las desventajas radica en realizar movimientos de muchos puertos, ya que se tiene que realizar la reconfiguración de todos los puertos individualmente; una tarea de este tipo se puede reducir considerablemente con el uso de una VLAN dinámica que identifica al equipo que se está conectando al switch. Para realizar una configuración y administración más sencilla de una red con cantidades superiores a 5 switches, por ejemplo, es necesario utilizar el protocolo VTP VLAN trunking protocol.

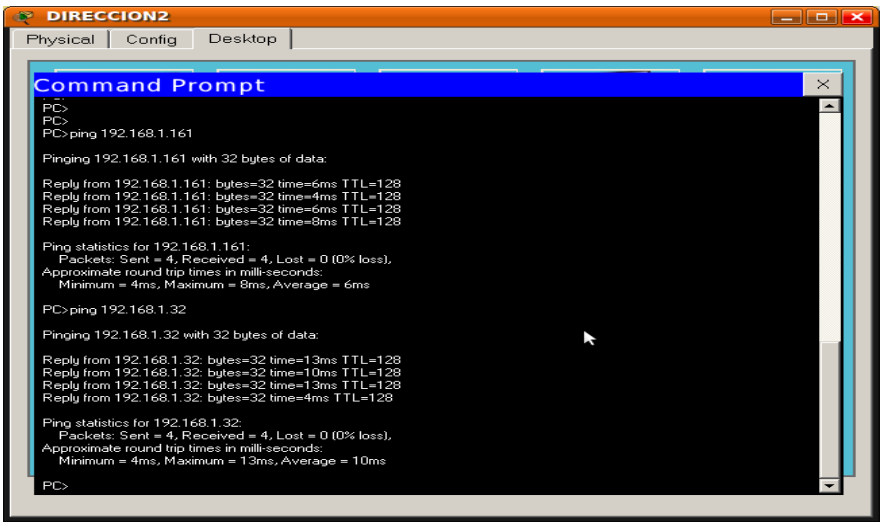
En el cual se define un servidor donde se pueden crear y modificar VLAN y éstas se ven reflejadas en los clientes, un cliente no tiene permitido crear borrar o administrar una VLAN, y un transparente tiene permisos de crear, borrar o administrar una VLAN localmente.

VTP permite las soluciones de red conmutadas que son fácilmente escalables a otras dimensiones. Cuando se utiliza más de una VLAN entre diferentes switches o routers, se necesita contar con un enlace troncal que funcione como conducto. Un puerto de enlace troncal con el protocolo IEEE 802Q admite tráfico etiquetado y sin etiquetar. Durante el diseño de una VLAN se recomienda que la nativa no sea de gestión, que se cambie de la que se tiene por defecto en la VLAN 1, que todos los switches se encuentren en la misma VLAN nativa y los usuarios y servidores en sus respectivas VLAN diferentes a la nativa, y que el tráfico entre switches no se encapsule dentro de los enlaces trunk. Con las VLAN creadas en la red, es necesario que éstas se comuniquen entre sí, por lo tanto es necesario realizar un enrutamiento entre las diferentes VLAN. Para lograr esto se utiliza la interfaz de un enrutador que se configura para funcionar como enlace troncal, con esto se acepta el tráfico etiquetado de una VLAN troncal y lo enruta de manera interna entre las VLAN. Esta tarea será realizada por el departamento encargado de administrar los routers de la red, que es la siguiente capa dentro del modelo OSI, la capa de red. Con esta sugerencia al momento de comunicarse VLAN diferentes el rendimiento de la red no se vería seriamente afectado ya que se conocerían los caminos por los cuales llegar de una a otra VLAN y no se enviaría información a innecesaria.

Con la estructura propuesta podemos asegurar que cada segmento de red asignada a su respectiva VLAN, el tráfico de la red se distribuye por los segmentos configurados y no se distribuye creando tráfico en otros segmentos.

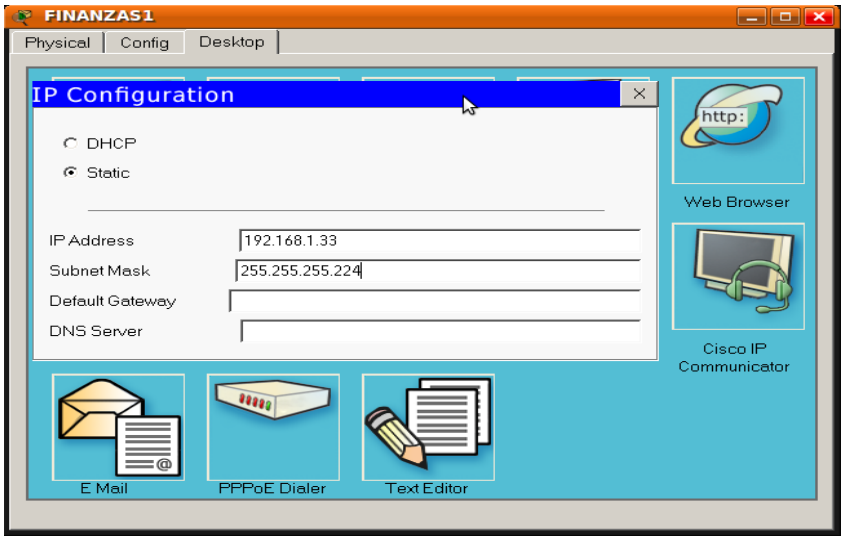
ANEXOS

Anexo 1



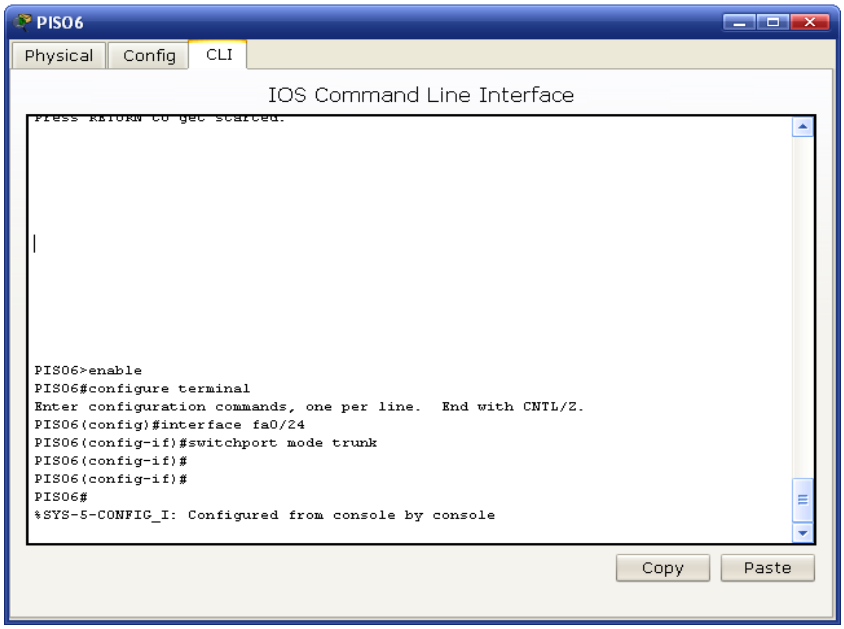
Comunicación antes de configuración

Anexo 2



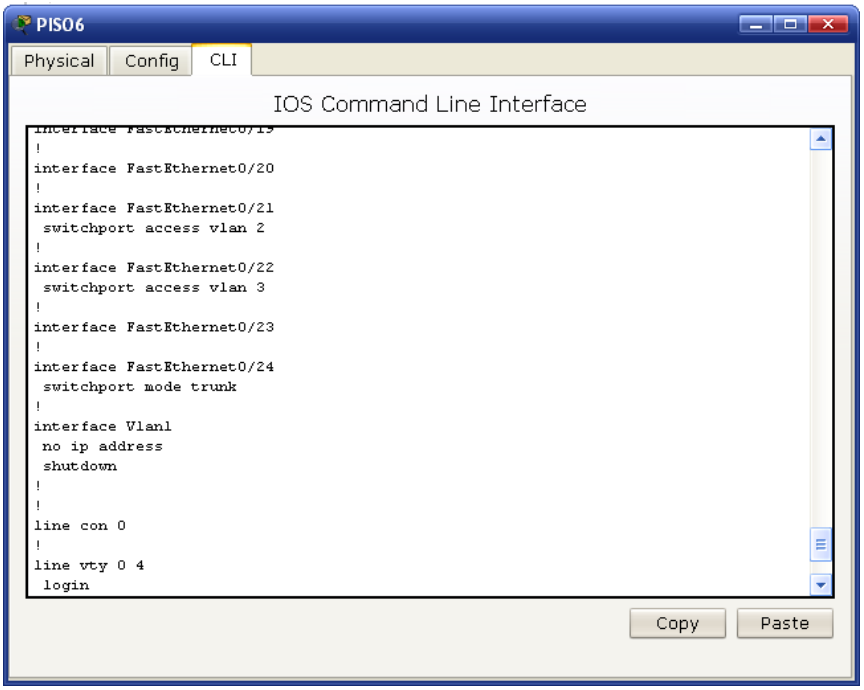
Asignación de IP a equipo de trabajo (PC)

Anexo 3



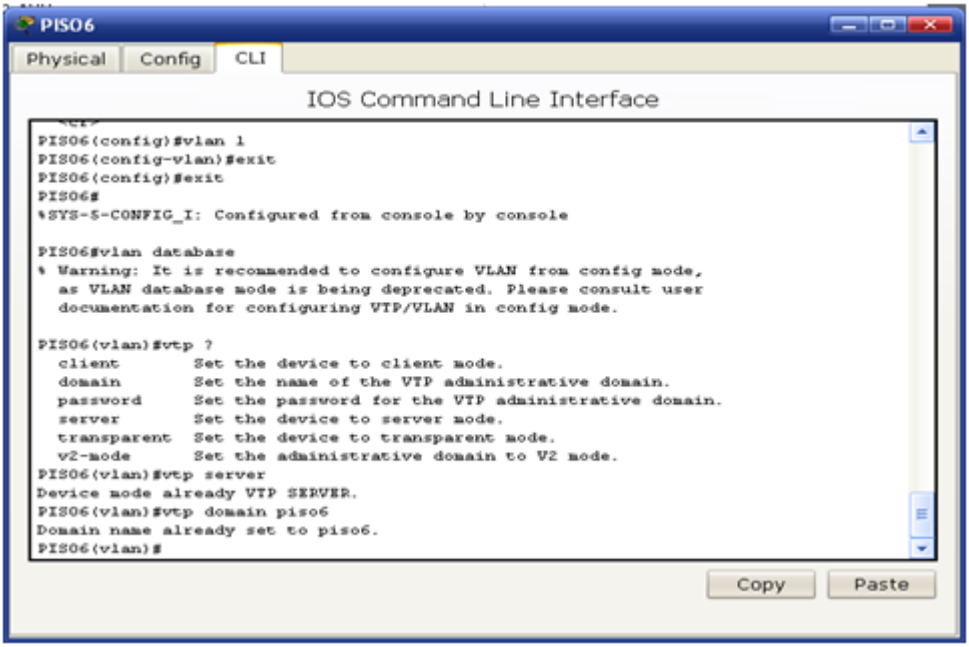
Configuración de enlace troncal en el switch

Anexo 4



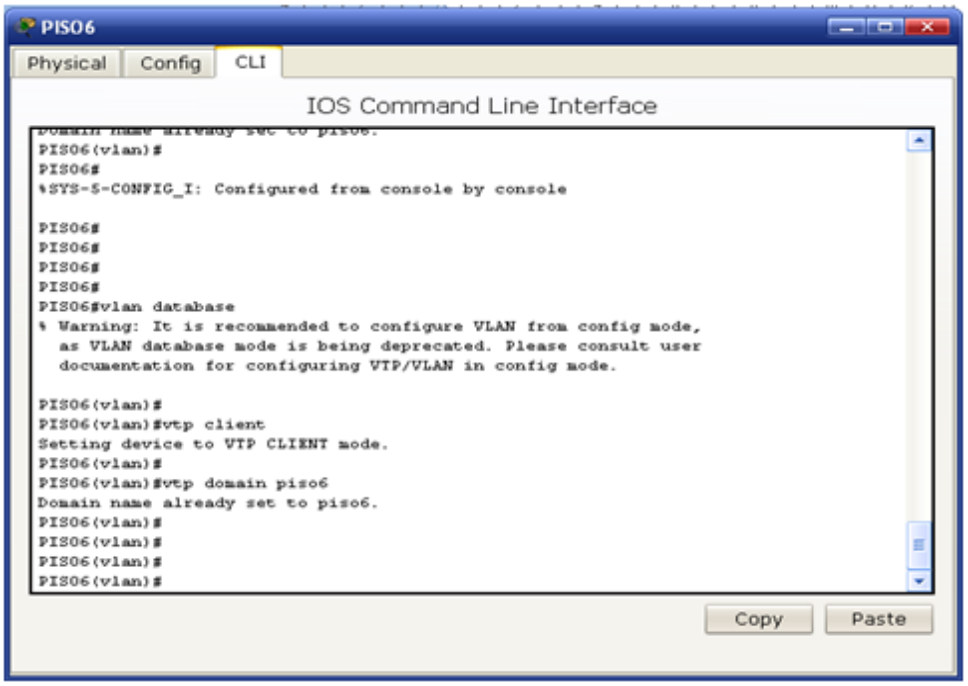
Utilidad del comando show running-config

Anexo 5



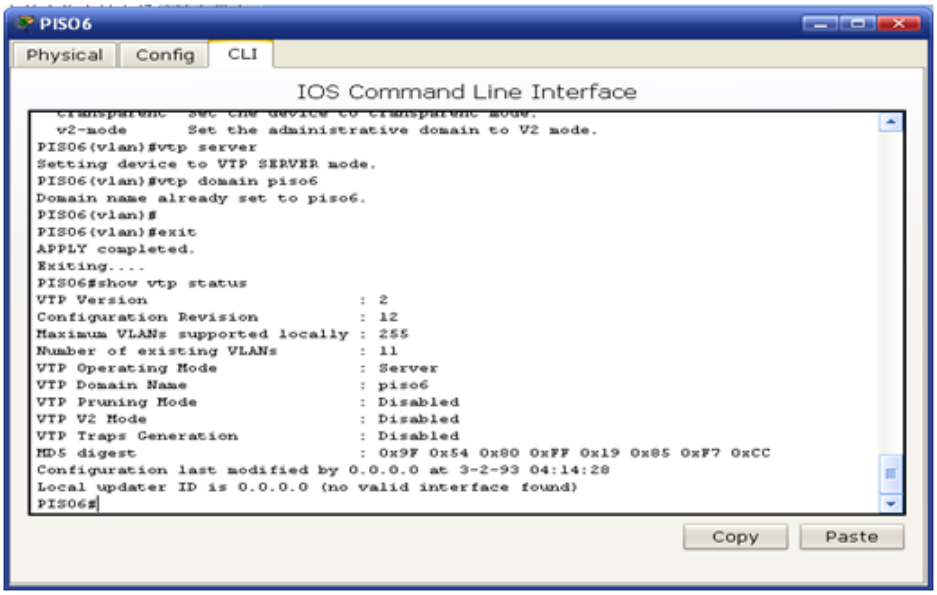
Configuración VTP modo SERVIDOR.

Anexo 6



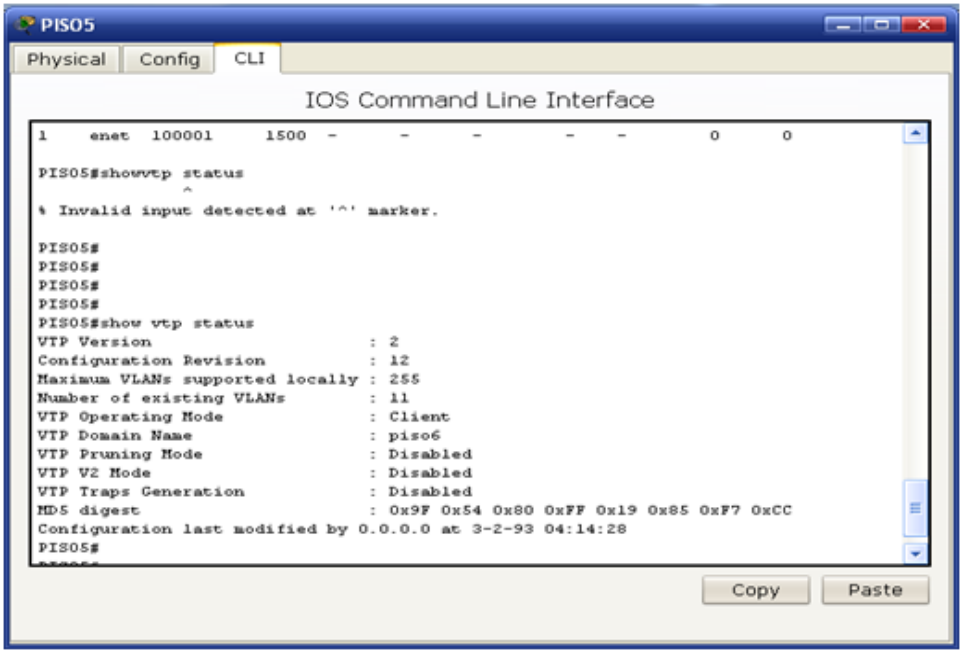
Configuración VTP en modo CLIENTE

Anexo 7



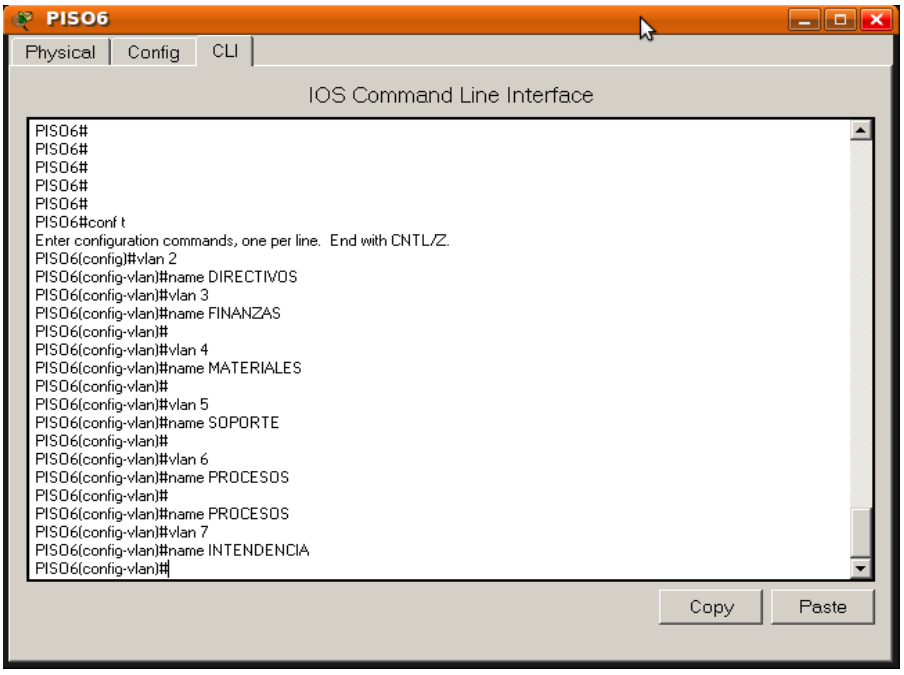
Estado de switch en modo SERVER

Anexo 8



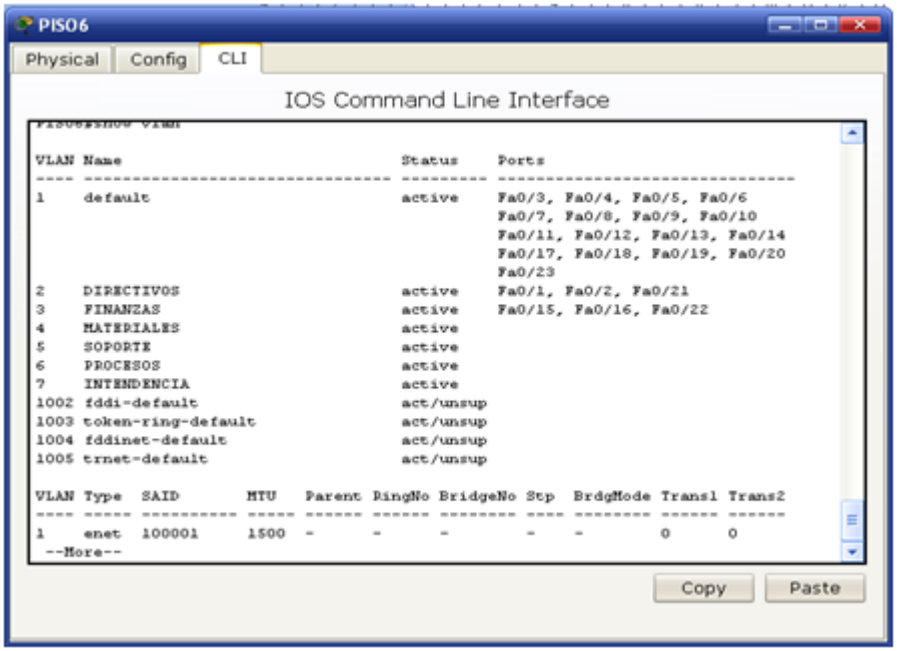
Estado de switch en modo CLIENTE

Anexo 9



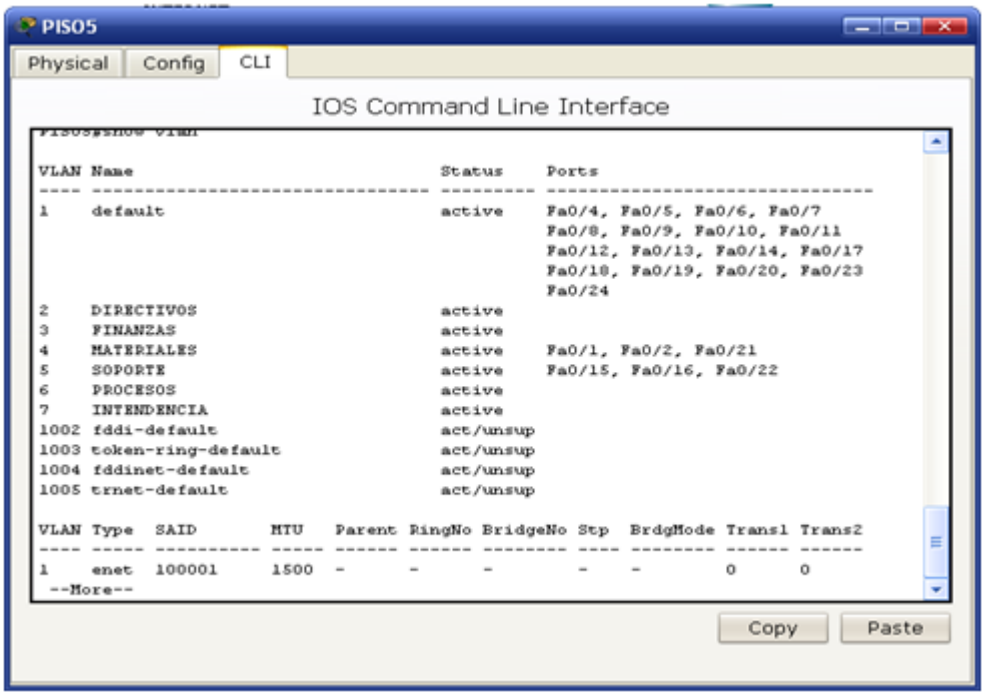
Creación y nombramiento de una VLAN

Anexo 10



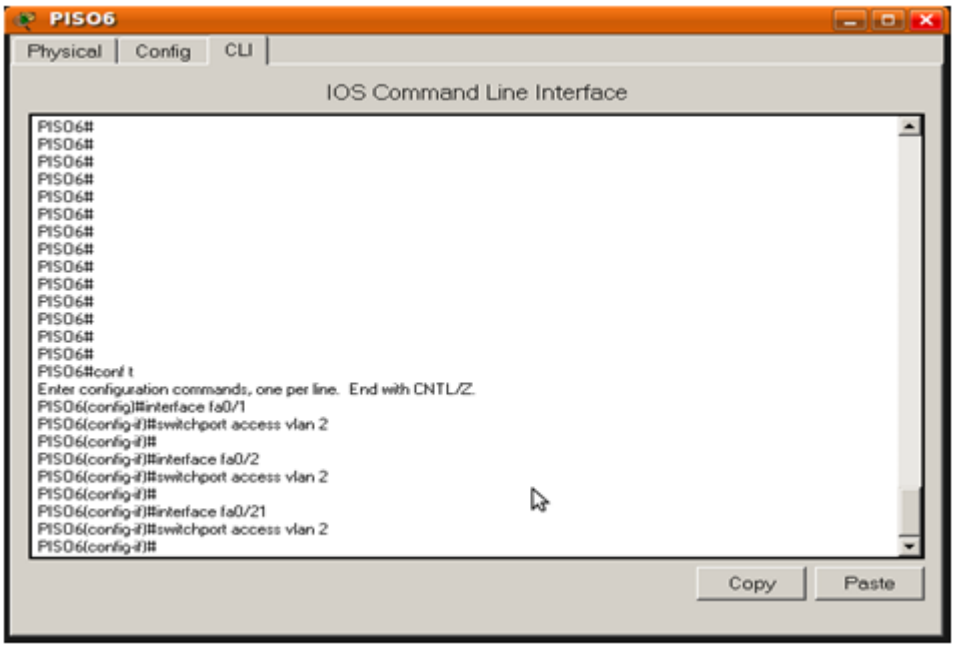
Utilidad del comando show VLAN

Anexo 11



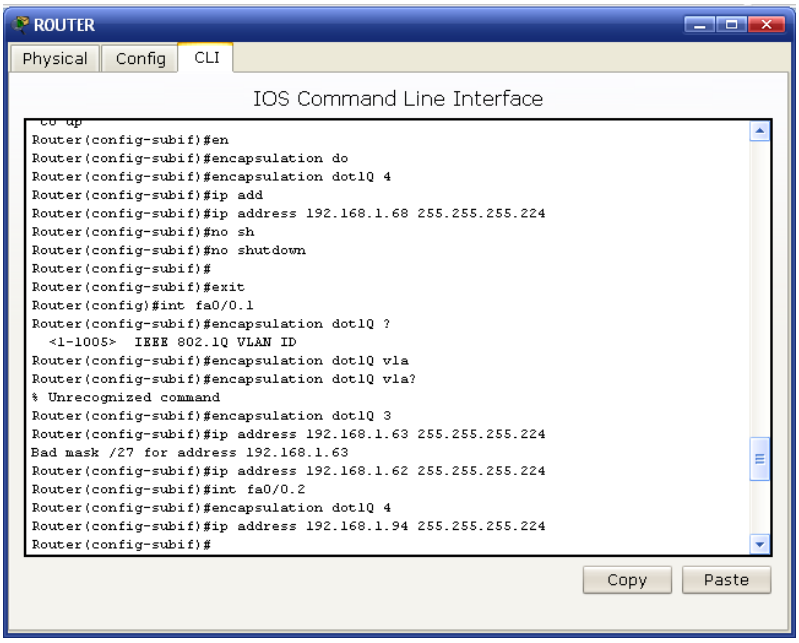
Visualización de VLAN en switches clientes

Anexo 12



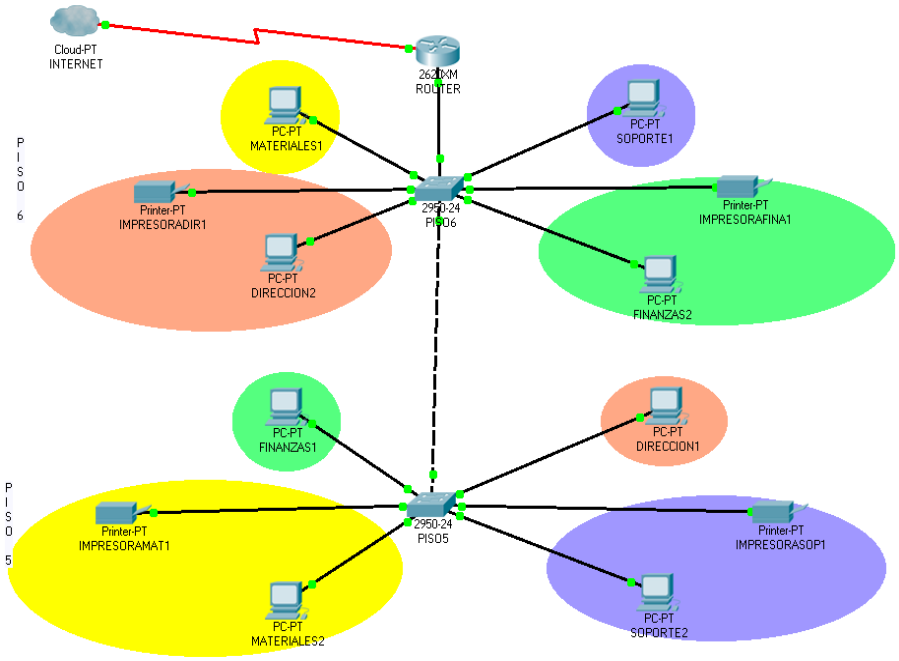
Asignación de puertos a VLAN's

Anexo 13



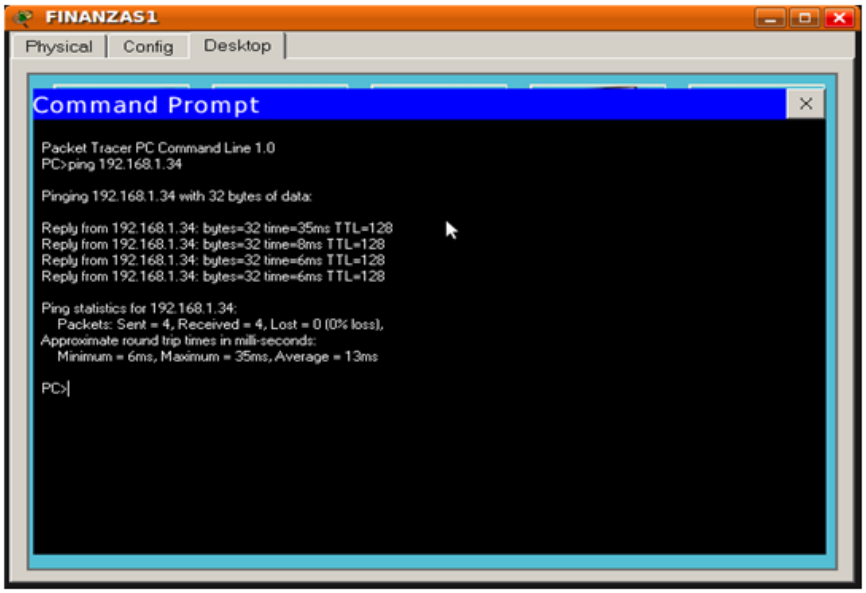
Visualización de configuración de inter VLAN en router.

Anexo 14



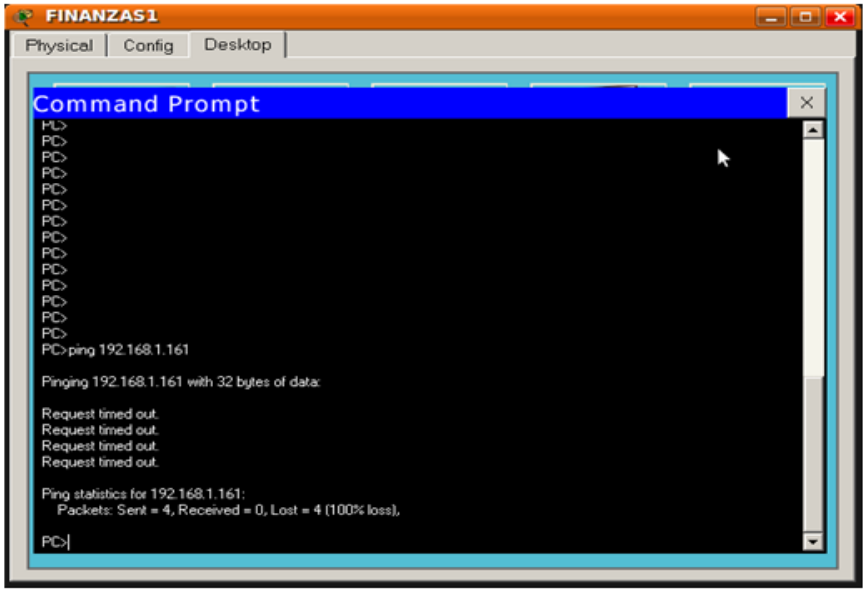
Red segmentada

Anexo 15



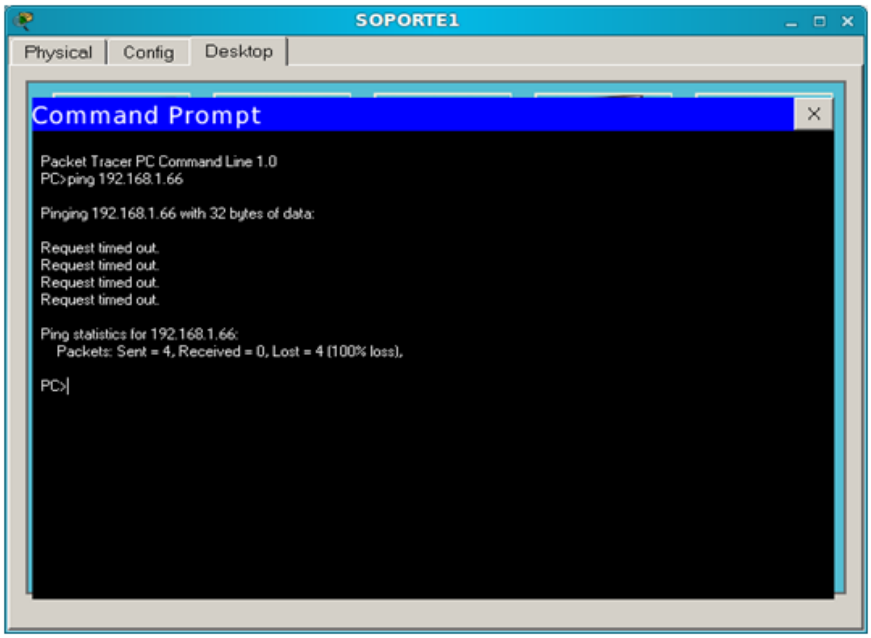
Comunicación entre PC de misma VLAN

Anexo 16



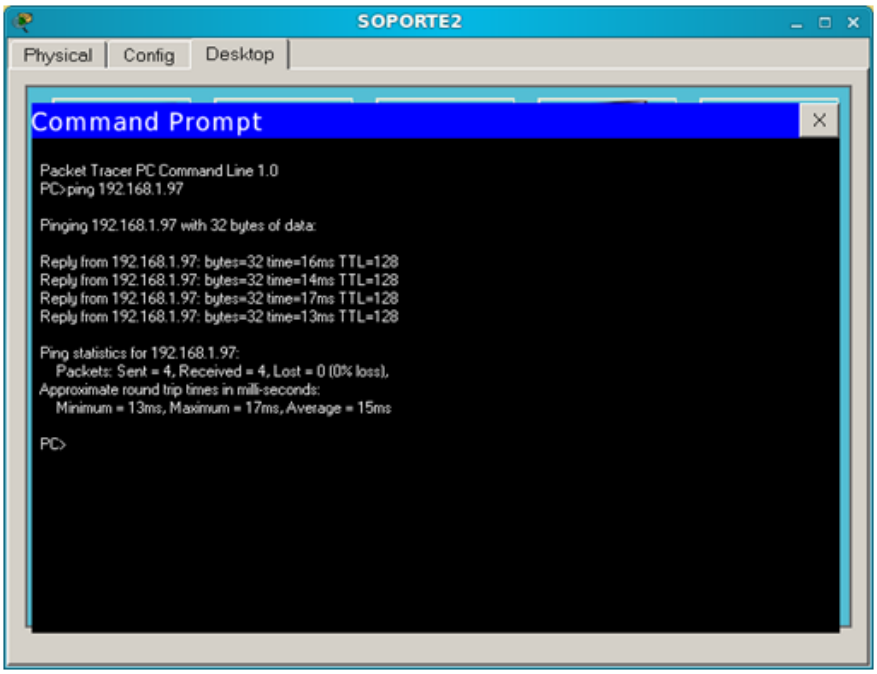
Comunicación negada a PC de Finanzas a PC de Directivos

Anexo 17



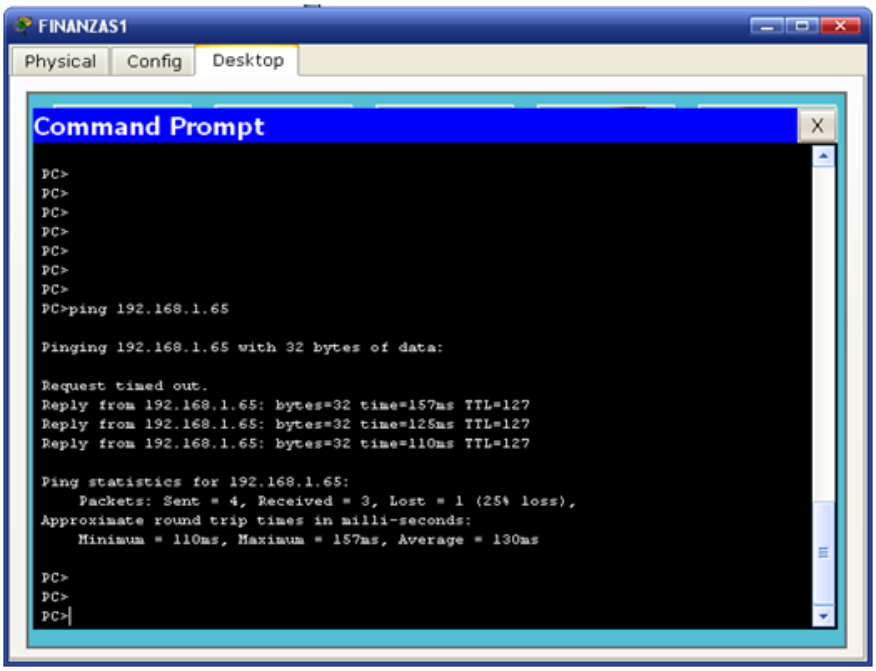
Comunicación entre VLAN Soporte – Materiales

Anexo 18



Comunicación entre VLAN Soporte

Anexo 19



Comunicación entre VLAN Finanzas – Materiales

ÍNDICE DE FIGURAS Y TABLAS

CAPITULO 1. REDES DE COMPUTADORAS

CAPITULO 2. VIRTUAL LAN

CAPITULO 3. SUBNETEO

CAPITULO 4. IMPLEMENTACIÓN DE GRUPOS DE TRABAJO POR MEDIO DE VLAN

GLOSARIO DE TÉRMINOS

Address: Dirección. Estructura de datos empleada para identificar una entidad única dentro de una red, que puede ser un dispositivo o un proceso.

Address mask: Máscara de dirección. Conjunto de bits empleados para definir las partes de la dirección que se refieren a la subred y a la estación o host.

Address MAC: (siglas en inglés de *media access control*; en español "control de acceso al medio") es un identificador de 48 bits (3 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red.

Aplicación: Programa de ordenador que ofrece servicios al usuario.

Binario: Sistema de representación digital de información en el que se definen solamente dos condiciones, que pueden estar representadas solamente de dos maneras.

Bit o dígito binario: Es un dígito del sistema de numeración binario. Es la mínima unidad de información, representada por una alternativa entre unos valores de señal a los que se hace corresponder el “uno” o el “cero”.

Bridge: Puente. Dispositivo de internetworking que procesa tramas entre segmentos de una red local en función de su dirección MAC.

Broadcast: Difusión. Valor del atributo de servicio de configuración de las comunicaciones que denota distribución unidireccional a todos los usuarios de una red.

Byte: Conjunto de elementos binarios que se maneja como una unidad. Los más comunes son de ocho bits u octetos.

Cable: Medio de transmisión, puede estar formado por hilos conductores o fibras ópticas envueltas mediante una cubierta protectora.

Canal: Término genérico para una vía de transmisión serie.

Cliente: Software empleado para establecer conexiones con objeto de intercambiar información con otro programa servidor, con el que está específicamente diseñado para poder trabajar.

Client-server: Cliente-servidor. Referencia en general a interacciones de petición/respuesta entre dispositivos procesos.

Coaxial: Cable formado por un conductor central axial rodeado de un conductor cilíndrico que hace de pantalla, estando separados ambos por un aislante.

Colisión: Es el método de acceso CSMA/CD, la colisión ocurre cuando dos dispositivos intentan transmitir simultáneamente, debiendo proceder a una retransmisión posterior en diferentes instantes de tiempo.

Comunicación: Transmisión de información.

Configuración de red: Topología y organización de red.

Conmutación de mensajes: Técnica que permite la transferencia de mensajes entre dos usuarios, encargándose la red de su almacenamiento intermedio y posterior envío.

Conmutación de paquetes: Técnica de envío de información en paquetes de datos, encargándose la red de su encaminamiento hasta el punto de destino.

Consola: Terminal conectado directamente a un host, que permite introducir comandos.

Datagrama: Paquete de datos que circula en la red sin conexión. Unida de información de nivel de red que se transmite a través de los medios de comunicación sin el establecimiento previo un circuitos.

Difusión: Transmisión simultánea de información desde una única fuente hacia múltiples destinatarios.

Dirección: Conjunto de números que identifican de forma única un dispositivo de red.

Encaminamiento: Determinación de la ruta a tomar en una red para una comunicación.

Enlace: Conexión que se establece a través de las líneas físicas de comunicación mediante los protocolos adecuados.

Estado de red: Define la situación en la que se encuentra una red de comunicación.

Ethernet: Es un estándar de redes de área local de computadoras.

Frame Relay: Es una técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual.

Gateway: Denominación normalizada de los dispositivos que permiten la interconexión de dos redes con arquitecturas distintas.

Host: Usado en informática para referirse a las computadoras conectadas a una red, que proveen y utilizan servicios de ella.

Hub: Concentrador. Es un dispositivo que permite centralizar el cableado de una red y poder ampliarla. Esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndola por sus diferentes puertos.

IEEE: Institute of Electrical and Electronics Enginieers. Organización que regula las normas que regulan la comunicación entre dispositivos.

Interface: Punto de demarcación o frontera en las que definen las características y procedimientos físicos y lógicos para el intercambio de información.

IP: Protocolo usado para la comunicación de datos a través de una red.

IPX: Intercambio de Paquetes Interred, se utiliza para transferir datos entre el servidor y los programas de las estaciones de trabajo.

Máscara de subred: Parámetro de configuración del protocolo IP que permite obtener la configuración de host y de red a partir de la dirección IP.

Megabit (**Mbit** o **Mb**)**:** Es una unidad de medida de información muy utilizada en las transmisiones de datos.

Mensaje: Grupo de caracteres y sus elementos binarios de control asociados, que son transmitidos como un todo desde un emisor hasta un receptor.

Multicast: Proceso por el cual se envía información a múltiples destinos a la vez.

Nodo: Dispositivo que esta conectado a la red y tiene una dirección definida, teniendo como función principal la de conmutación, de circuitos o de mensajes.

Octeto: Es un grupo de ocho bits.

Ofimático: Es el equipamiento entre hardware y software usado para crear, coleccionar, almacenar, manipular y transmitir digitalmente la información necesaria en una oficina.

OSI o modelo de interconexión de sistemas abiertos: Es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

Paquete: Bloque de información identificado por una etiqueta de nivel de red.

Protocolo: Es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red.

Protocolo de comunicación: Conjunto de reglas para establecimiento, mantenimiento y cancelación de conexiones que permite la transferencia de datos entre dos o más dispositivos.

Recursos: Los recursos vienen dados por las capacidades que tiene los elementos que forman un sistema de comunicaciones para la realización de sus actividades.

Red: Conjunto de nodos interconectados por líneas de transmisión, y cuya función es la de que los elementos a ella conectados puedan establecer una comunicación.

Router: Encaminador. Dispositivo hardware o software para interconexión de redes de computadoras que opera en la capa de red de datos del modelo OSI.

Sincronización: Mecanismo por el que el reloj del receptor se ajusta al del transmisor.

Subred: Es un rango de direcciones lógicas.

Switch o conmutador: Es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa de enlace de datos del modelo OSI.

TCP/IP: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), el conjunto de protocolos de red en la que se basa Internet o intranet.

VLAN Virtual Local Area Networks, Red de Área Local Virtual.

BIBLIOGRAFÍA

- Ariganello Ernesto: “Guia de estudios para la certificación CCNA – 640 – 801”Editorial Alfaomega – Ra-Ma 2007.
- Cisco Systems. “Guia del primer año. CCNA 1 y 2”. Tercera edición. Editorial CiscoPress 2003
- Cisco Systems. “Guia del primer año. CCNA 3 y 4”. Tercera edición. Editorial CiscoPress 2003.
- Academia de Networking de Cisco Systems “Guía del Segundo Año”, Tercera Edición, Editorial Pearson Education, Madrid 2004.
- Tanenbaum, Andrew S.: “Redes de computadores”. Tercera edición. (pag. 423-433)
- Derfler, Frank.: “Descubre redes LAN y WAN”. Prentice Hall, 1998.
- Parnell, T.: “LAN Times Guía de redes de alta velocidad”
- W. Stallings.: "Comunicaciones y Redes de Computadores", 7ª edición, Pearson/Prentice-Hall, 2004.
- David Passmore y John Freeman, "The Virtual LAN Technological Report"
- Varadarajan, S.: “Virtual Local Area Networks”
- Passmore, D.; Freeman, J.: “The Virtual LAN Technology Report”

CIBEROGRAFÍA

- http://www.textoscientificos.com/redes/redes-virtuales
- http://www.lcc.uma.es/~eat/services/rvirtual/rvirtual.html
- http://es.kioskea.net/contents/internet/vlan.php3
- http://www.ciscoredes.com/tutoriales/65-vlan.html
- http://www.garciagaston.com.ar/verpost.php?id_noticia=94
- http://www.redesymas.org/2011/04/intervlan-routing.html
- http://www.slideshare.net/alexgrz81/subneteo-de-redes
- http://www.monografias.com/trabajos11/inter/inter.shtml
- http://www.slideshare.net/Betty77ma/colisiones-dominios-de-colisin-y-segmentacin
- http://www.alegsa.com.ar/Dic/red%20de%20computadoras.php
- http://www.redesymas.org/2011/04/manual-de-comandos-basicos-de-switches.html
- http://programoweb.com/71653/implementacion-de-vtp/
- http://www.the-evangelist.info/2010/03/ccnp-switch-5-vlan-trunking-protocol/
- http://www.lcc.uma.es/~eat/services/rvirtual/rvirtual.html
- http://inf.udec.cl/~yfarran/web-redes/ind-redes.htm
- http://coqui.metro.inter.edu/cedu6320/mlozada/menu2.htm
- http://redesafull.galeon.com/
- http://www.gta.ufrj.br/grad/98_2/fernando/fernando.html
- http://www.ciscopress.com/articles/article.asp?p=29803
- http://www.axis.com/es/products/video/about_networkvideo/vlan.htm