TECNICAS DE OPTIMIZACION Y MEJORAMIENTO DE UNA RED LAN EMPRESARIAL

EDWIN ALFONSO GONZALEZ PIÑERES

HERNAN DARIO SERRANO MAYORGA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

ESPECIALIZACIÓN EN TELECOMUNICACIONES

JUNIO DEL 2011

CARTAGENA

TECNICAS DE OPTIMIZACION Y MEJORAMIENTO DE UNA RED LAN EMPRESARIAL

EDWIN ALFONSO GONZALEZ PIÑERES

HERNAN DARIO SERRANO MAYORGA

Monografía presentada como requisito para optar al título de Especialistas en Telecomunicaciones

DIRECTOR

ING. GONZALO LÓPEZ VERGARA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

ESPECIALIZACIÓN EN TELECOMUNICACIONES

JUNIO DEL 2011

CARTAGENA

TABLA DE CONTENIDO

Pág.

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

Desde el inicio de los tiempos el hombre ha implementado diferentes medios para la transmisión de información. Desde métodos totalmente manuales como el sistema de correo escrito, pasando por el telégrafo, el teléfono hasta llegar hoy en día al envío y recepción de información de manera digital por medio de redes.

En el sector empresarial las comunicaciones son parte fundamental de su funcionamiento, por ello es necesario poder conocer e implementar soluciones de comunicaciones que ayuden al funcionamiento, buen uso y mantenimiento de las comunicaciones dentro de las empresas; por medio del estudio de las redes LAN empresariales.

Referirnos a la comunicación de datos, es un proceso común y cotidiano, que en ocasiones, hasta para aquellas personas distanciadas del mundo de la computación caen en la necesidad de manejar y transmitir información.
Pero en ocasiones el manejo y la transmisión de los datos resulta distorsionada, por lo que los usuarios deben asegurarse que sus datos se entreguen y reciban de manera adecuada, en el sector empresarial, este problema es aun más evidente e importante de controlar, debido a que de esas comunicaciones depende el buen funcionamiento de la empresa.

Para poder iniciar correctamente con un proceso de mejoramiento de las comunicaciones de datos en una red LAN empresarial, es necesario poder determinar los errores que esta posee y de esa manera implementar la solución más acorde con las necesidades.

En la actualidad para las empresas, las redes digitales son de vital importancia y en un mundo tecnológico donde todo se moviliza hacia la automatización y la digitalización; un problema en las comunicaciones; se ve reflejado económicamente en perdidas hacia la empresa. Por esta razón es de vital importancia poder encontrar, solucionar y ante todo prevenir; los problemas que se puedan generar en una red LAN empresarial.

1. HERRAMIENTAS PARA VERIFICACION LAN EMPRESARIAL

Existen diferentes herramientas tanto de Hardware como de Software para la verificación del funcionamiento de una red LAN empresarial y para la identificación de posibles daños o errores que esta pueda tener.

1.1 HERRAMIENTAS HARDWARE

Normalmente la mayoría de las fallas que se pueden presentar en una red LAN empresarial corresponden a los errores o daños físicos, estos errores vienen dados por problemas en el medio de transmisión.
Para determinar problemas en el medio de transmisión el orden correcto es iniciar con una verificación física. Con esto se quiere decir que se debe verificar:

Si el medio de transmisión es el apropiado
Si los conectores son los correctos y se encuentran correctamente ponchados.
Si se encuentran correctamente conectados los equipos.
De estar correctamente conectados si muestran link en la conexión.

Finalizada esta verificación se debe proceder a una verificación del medio. Existen diferentes equipos para la verificación de los diferentes medios de transmisión. Los de cobre sean Coaxial o UTP, en los cuales se trasmite señales eléctricas; y los Ópticos para realizar medidas de la luz y potencia de esta en la fibra óptica.

1.1.1 Tester de Red

Para la verificación de los cableado de cobres se utilizar un verificador o Tester de cableado, en este se puede realizar verificación del cableado sea coaxial o UTP. Con esta herramienta de Hardware se puede diagnosticar cual es el problema que presenta el cableado.
Puede verificar si el cableado posee continuidad, se encuentra abierto, en cortocircuito o si el cable se encuentra con pares cruzados.
A continuación podemos observar un ejemplo de un equipo verificador de cableado UTP y Coaxial.

Figura 1. Tester de Red

1.1.2 Power Meter

Si el medio de transmisión, corresponde a Fibra Optica, se pueden utilizar una herramienta conocida como Power Meter, como su nombre lo indica mide la potencia de luz en Dbm con que llega al punto de medición, estos valores deben estar entre el rango de sensibilidad del equipo receptor.

Con esta herramienta podemos determinar si la fibra se encuentra atenuada, si posee alguna ruptura o problema en los empalmes; esto se realiza midiendo la potencia de luz transmitida y la potencia de llegada; pero no se puede determinar el lugar donde se presenta el inconveniente.

A continuación podemos observar un ejemplo de power meter, el cual nos muestra una potencia de -11.39 dbm.

Figura 2. Power Meter

1.1.3 OTDR (Optical Time Domain Reflectometer)

El OTDR es otra herramienta muy útil para la verificación de la fibra; nos permite no solo medir la potencia, sino también poder analizar todo el funcionamiento de la fibra óptica; esta herramienta nos permite determinar un daño en fibra, mostrando todos los eventos de la transmisión.

A continuación podemos observa un ejemplo de un OTDR.

Figura 3. Equipo OTDR

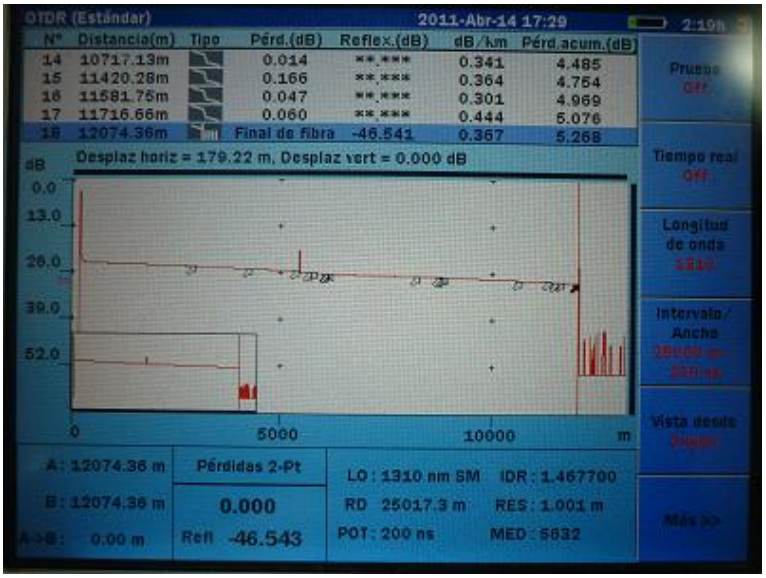

Figura 4. Análisis Fibra con OTDR

En la figura 4 podemos observa un OTDR en funcionamiento, en el se muestran los eventos y perdidas de potencia a lo largo del trayecto de fibra con esto se puede diagnosticar si se tiene algún problema; podemos observar nos muestra las perdidas por atenuación producidas por los empalmes de fibra, a lo largo de todo el recorrido y la distancia total de la fibra.

De no posee ninguna herramienta para la verificación del medio, se debe hacer la conexión de los equipos como deben funcionar normalmente y verificar que los equipos conectados den link; siempre al estar conectados 2 equipos correctamente se muestra un indicador led, el cual informa que existe una conexión física establecida.

1.2 HERRAMIENTA SOTFWARE

Existes muchas herramientas de software para ayudarnos a encontrar errores y mejorar el funcionamiento de una red LAN empresarial, explicaremos las más utilizadas.
La herramienta más conocida y utilizada para verificar un enlace, es el comando PING, este se realiza desde la ventana de símbolo del sistema.

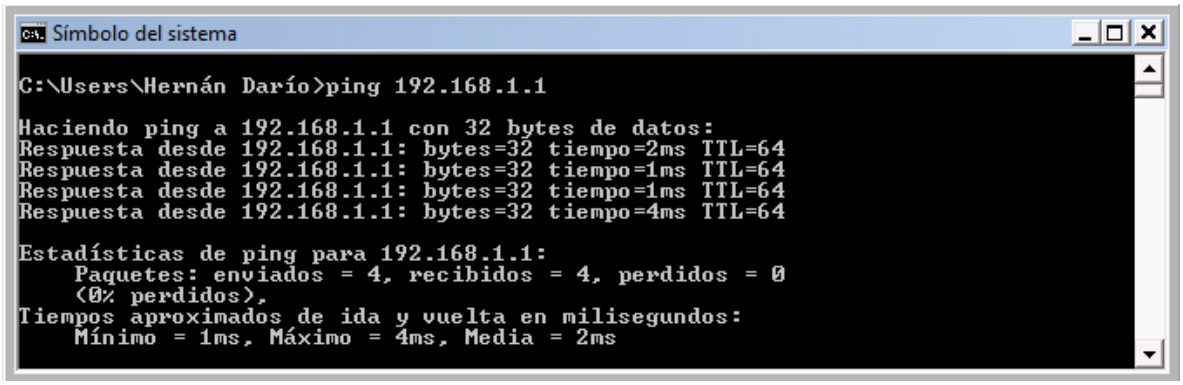

Figura 5. Prueba de Ping

En la figura 5 podemos observar un ejemplo del funcionamiento del comando ping desde un PC.
El comando ping realiza una petición de respuesta a una dirección IP destino, en el caso del ejemplo la 192.168.1.1.
De ser una respuesta positiva quiere decir que se posee conexión correctamente con la IP seleccionada. Se puede verificar los tiempos de respuesta para determinar si hay problemas de pérdida o retraso de paquetes en la transmisión.

De haber problemas o la respuesta es negativa se puede verificar con el comando Trace.

El comando TRACERT, nos permite trazar una ruta, la cual nos muestra los saltos que tiene que hacer el paquete IP para llegar a su destino.
Es un comando muy útil para identificar en que tramo o que parte se encuentra el problema.

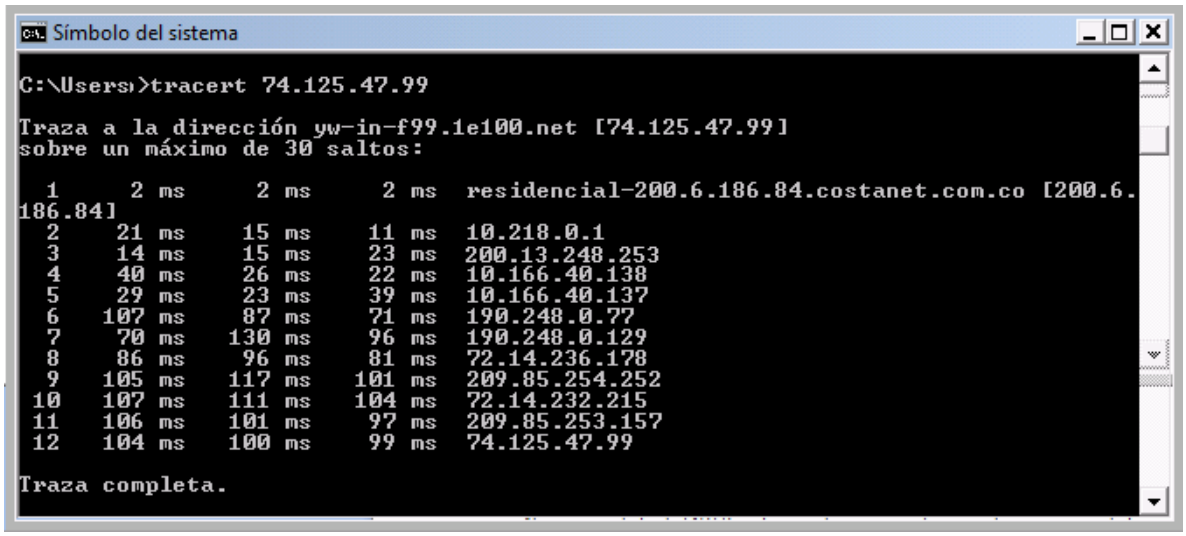

Figura 6. Prueba Trace route a página Internet

Este comando se recomienda si el ping no es exitoso, en la figura 6, podemos observar todos los saltos que hace el paquete IP por las diferentes redes antes de llegar a su destino.
Cuando existe un problema solo nos aparecen asteriscos (***).

Si se posee acceso al router o al switch un comando que nos puede ayudar a verificar las conexiones es el comando **show interface description.**

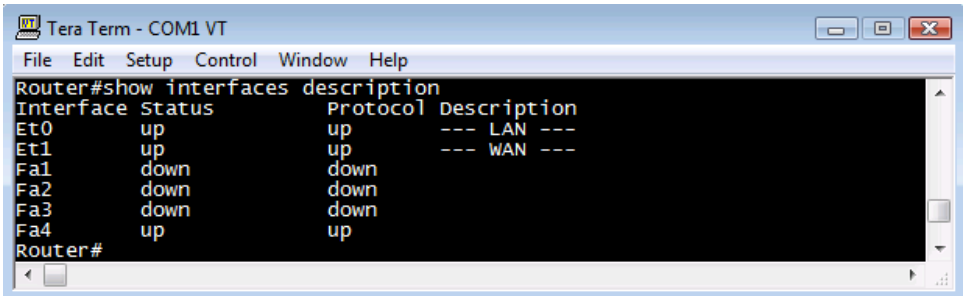

Figura 7. Comando Show Interface Description

En la figura 7, se muestra que se encuentra una columna de Status y otra de Protocolo. La primera nos muestra si la interface esta activa o apagada administrativamente. La segunda nos muestra si el protocolo está arriba, cuando el protocolo se encuentra en down, es debido a que no existe compatibilidad de protocolo en la interconexión de los equipos, para que funcionen correctamente se requiere que ambos equipos trabajen sobre el mismo protocolo; un error muy común es que no se encuentren igual el tipo de transmisión sea half o full dúplex y la misma velocidad de transmisión sea 10, 100 o 1000. Se requiere para su correcto funcionamiento que tanto el status de la interface como el protocolo se encuentra arriba (UP).

Para la verificación del enrutamiento se reqiere estar dentro de la consola del router y utilizar el comando **Show ip route.**

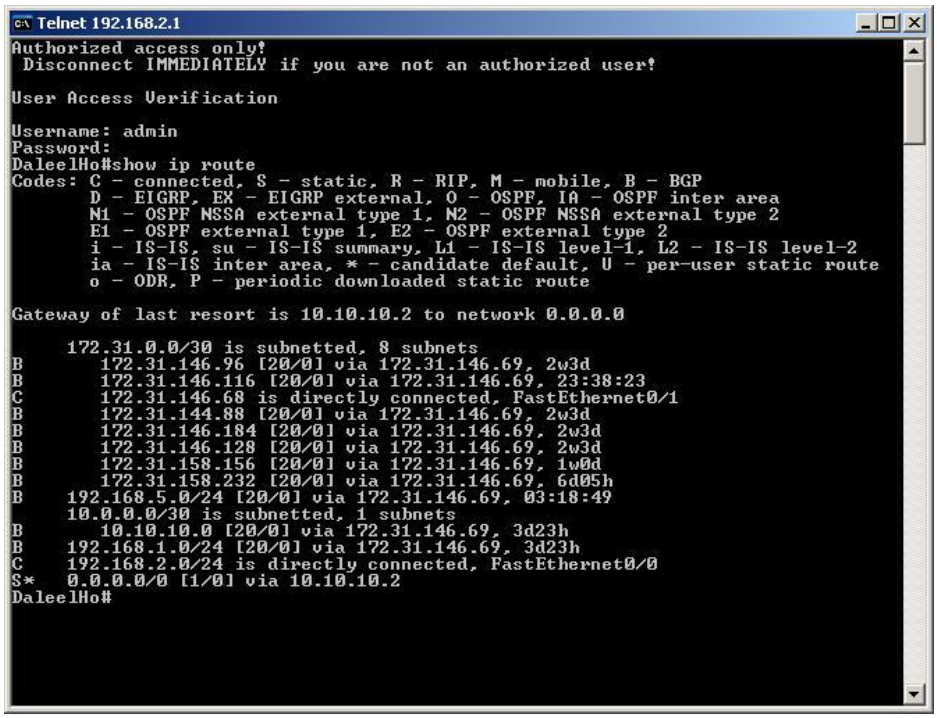

Figura 8. Comando Show Ip route

Como se muestra en la figura 8, el comando show ip route nos permite verificar el correcto funcionamiento del enrutamiento en el router; en el podemos observar una tabla con las rutas aprendidas, y por medio de que Ip o interface se llega a esa red; en la parte superior aparece el código en letra que corresponde al tipo de protocolo por el cual está aprendiendo la ruta, sea estática o dinámica como Bgp, Ospf, Eigrp etc.

1.2.1 Programa Sniffer

Existen también diferentes herramientas en la capa de aplicación que nos permiten verificar el correcto funcionamiento de la red LAN empresarial.

Una de estas herramientas son los programas conocidos como Sniffer.

Estos programas permiten realizar un monitoreo del trafico de la red LAN, mostrándonos el trafico de cada IP; de esta manera se puede determinar que IP está generando un tráfico fuera de lo normal o está consumiendo la mayoría del ancho de banda de la red.
A continuación se observa un ejemplo de un programa Sniffer llamado Capsa 7, existen infinidades de programas de este tipo que pueden ser descargados desde internet para la verificación de la red LAN.

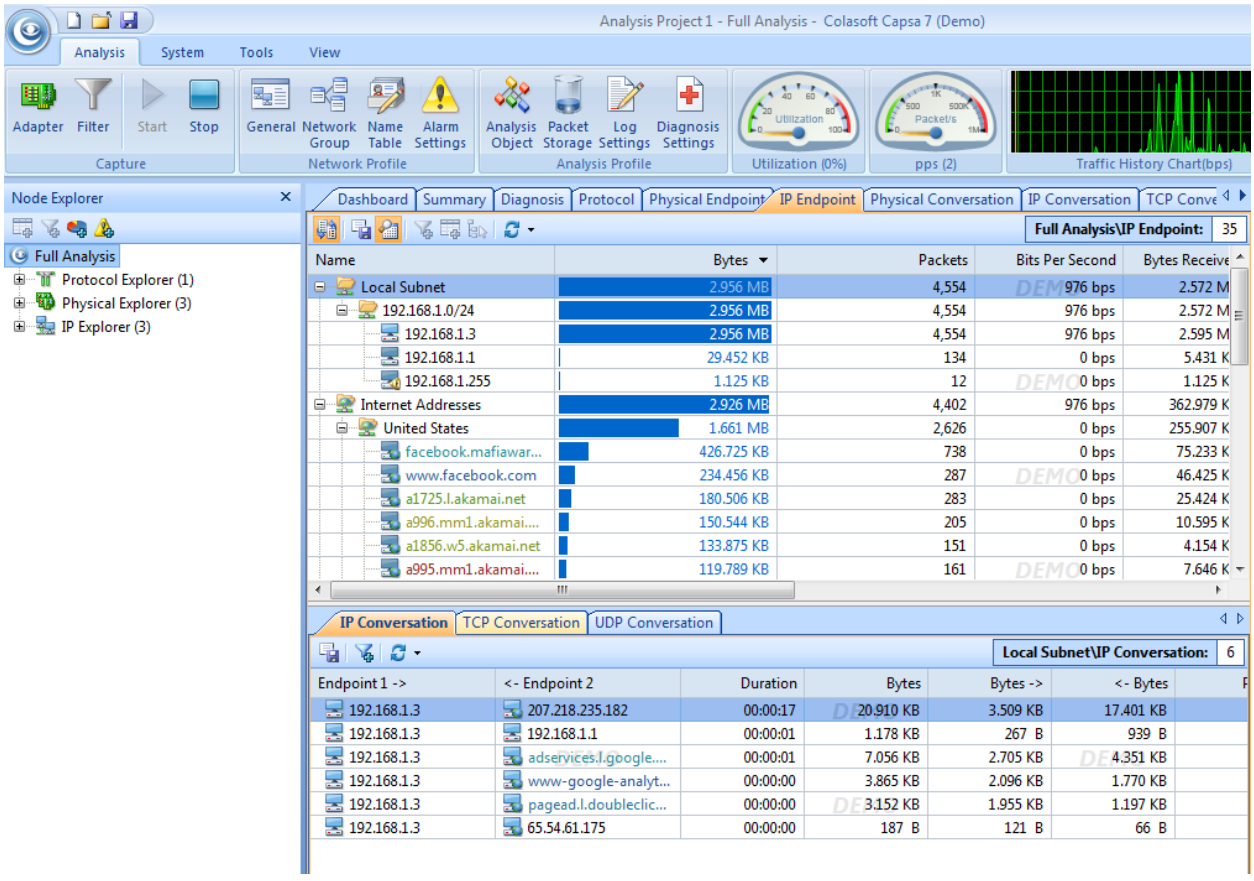

Figura 9. Pantalla funcionamiento Sniffer

En la figura 9, podemos observar cómo funciona el programa el cual nos muestra una lista de direcciones IP con sus consumos en bytes.

Se puede verificar los protocolos que se utilizar, las páginas más visitadas, estadísticas de tráfico entre otros elementos.
Es una herramienta muy útil para monitorear el consumo de la red LAN empresarial.

1.2.2 Programa Network View

Otra herramienta de software muy útil son los visores de red, en estos nos muestra el esquema completo de nuestra red LAN, todos los equipos que se encuentran conectados y lo hace de manera grafica lo cual nos ayuda a poder administrar y monitorear una red LAN empresarial, de esta manera podemos observar cuando se desconecta un equipo; un ejemplo de este tipo de software es Network View.

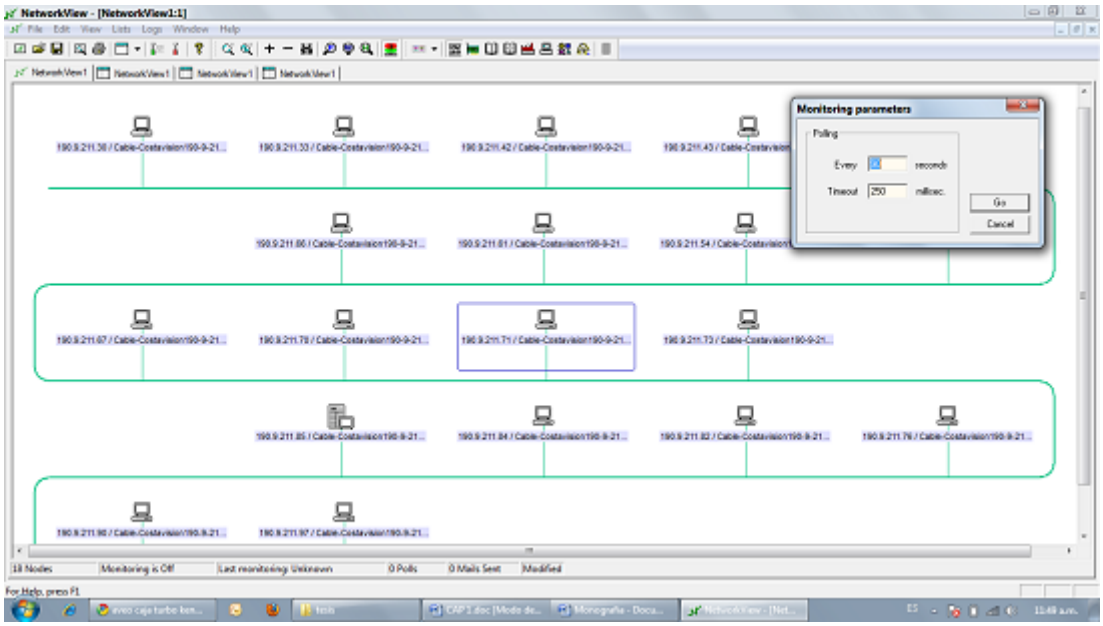

Figura 10. Funcionamiento Network View.

En la figura 10, podemos observar el funcionamiento del software Network View el cual nos creo la topología de una red LAN, en base al rango de IP que se asigno inicialmente; en esta herramienta se puede colocar los tiempo de monitoreo y generar alarmas si equipos primordiales como servidores se desconectan.

1.2.3 Firewall

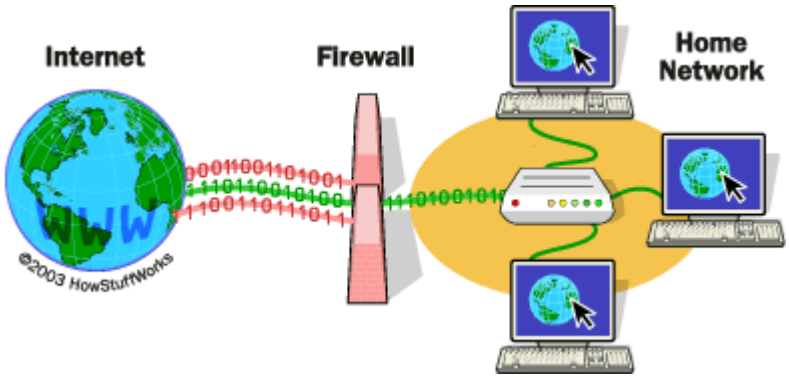

Figura 11 Funcionamiento Firewall.

El firewall es una herramienta la cual nos permite filtrar la información de entrada y de salida a nuestra red LAN empresarial desde Internet como se muestra en la figura 11.

Es importante para su correcto funcionamiento que el firewall este ubicado entre la conexión a Internet y la red LAN empresarial, debido a que el firewall no puede filtrar y por ende proteger la red de la información que no pase por él.

Se configura asignando reglas de entrada o salida de información, pueden ser de aplicativos, de datos y hasta de puertos.
Este sistema bloquea o permite la entrada o salida de la información; esto ayuda sustancialmente a la seguridad en la red empresarial.

Un firewall bien configurado permite que todo opere correctamente y que sea poco probable que los equipos de la empresa sean atacados por span o por virus desde la red externa de la empresa, también permite optimizar la red LAN permitiendo solo los accesos requeridos por los diferentes departamentos de la empresa y de esa manera no se malgaste ancho de banda ni recursos, en información sin importancia para las necesidades de la empresa.[1]

En la configuración del Firewall, se puede asignar reglas a los perfiles o usuarios de los equipos de la empresa; de esa manera se pueden tener diferentes niveles de acceso a Internet, en los diferentes departamentos de la red LAN empresarial.

[1] http://www.howstuffworks.com/firewall.htm

Se pueden crear grupos ejemplo el grupo de ventas solo debe tener acceso al aplicativo de ventas y no a los aplicativos de ingeniería y diseño; o a la página de Internet de proveedores solamente; todos esos accesos se configuran en las reglas de entrada y salida del Firewall.

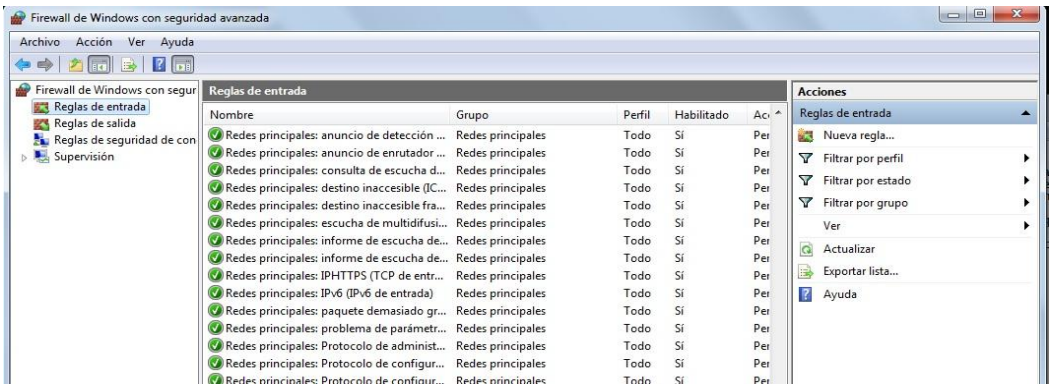

Figura 12 Ventana principal Firewall

En la figura 12, podemos observar la ventana principal que nos muestra el firewall al abrirlo; esta puede variar dependiendo de la versión del sistema operativo o tipo de sistema operativo, o del equipo utilizado para firewall.

En la parte izquierda se puede ingresar a las reglas de entrada o de salida y en la ventana del medio nos muestra cuáles de estas reglas se encuentran activas o desactivadas. Existen muchas reglas preestablecidas de las cuales podemos escoger cuales se dejarían activas y cuales desactivadas.
De ser necesario se pueden crear nuevas reglas; para generar una nueva regla de entrada o salida, se ingresa al generador de regla como se muestra en la figura 13, o administrador de regla y escogemos si es de entrada o de salida.

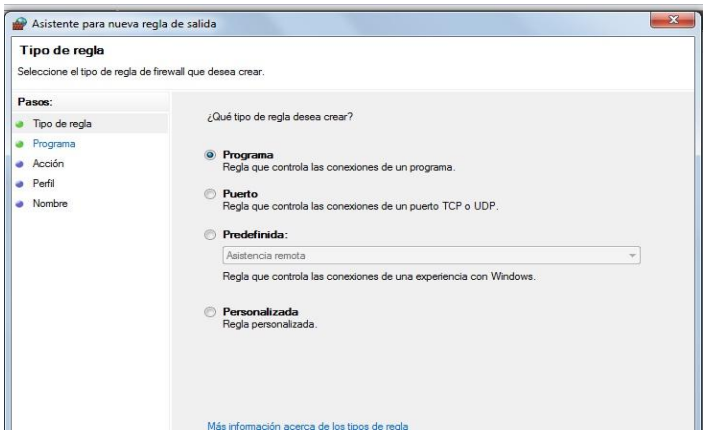

Figura 13 Generador de Regla Firewall

En esta ventana podemos encoger entre 4 opciones, se recomienda ingresar a la opción personalizada, para poder crear una regla con todos los parámetros de acceso.

Al señalar personalizada podemos escoger los parámetros a bloquear o permitir en nuestra red, se puede elegir si es un programa un puerto una acción; se puede asignar el tipo de protocolo a bloquear o habilitar los puertos, o se puede dejar por defecto todo depende de las necesidades que se requieran.
Para la aplicación de la regla se ingresa la IP o IPs dependiendo de las necesidades a las cuales se debe aplicar la regla como se muestra en la figura 14.

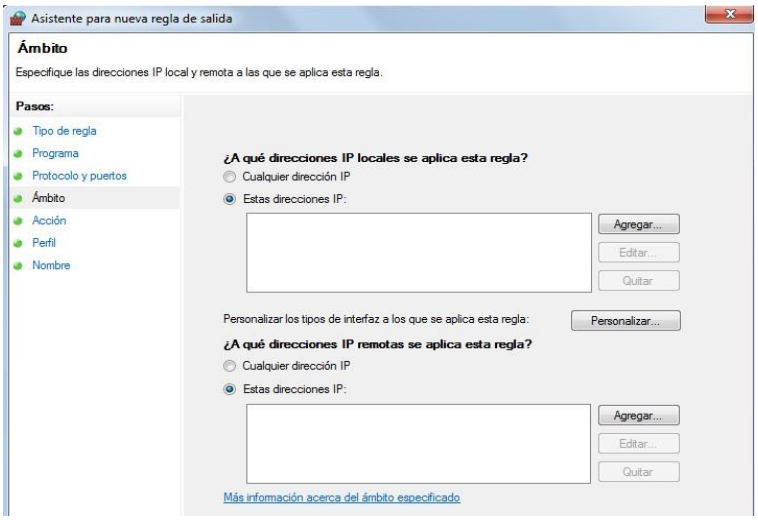

Figura 14 Aplicación de la regla

Se puede aplicar la regla a ciertas direcciones locales de nuestra red o que se bloquee entrar a ciertas direcciones en otras redes o Internet.

2. IMPLEMENTACION SPANNING TREE

En las redes LAN empresariales es muy común que los equipos tengan o requieran redundancia, esto quiere decir que posean más de una línea de comunicación lo cual permite que cuando la línea principal falle se cuente con otra o otras; de respaldo y así no se vea afectado el servicio.
Se puede decir que en una empresa Redundancia = Confiabilidad.

Cuando se tienen sistemas críticos que tienen que estar disponibles y funcionando, hay que intentar minimizar los fallos que puedan afectar al funcionamiento normal del sistema. De esta manera se pueden tener 2 caminos distintos, para llegar a un mismo destino por si alguno de estos fallara.

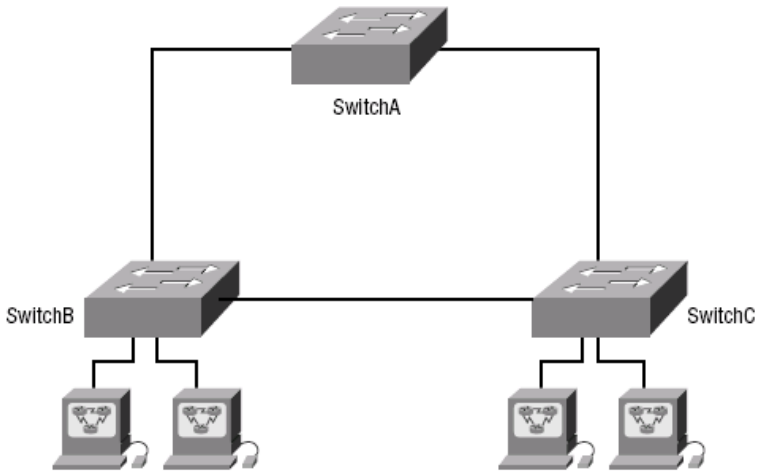

Figura 15. Red Redundante.

La redundancia genera un gran problema en los switch; debido a que si un nodo puede tener varias rutas alternativas para llegar a otro; un Switch tendrá problemas para aprender su dirección ya que aparecerá en dos de sus entradas. A esto se le llama “loop”. Para la solución de este problema se creó el protocolo Spanning Tree, su función principal es permitir rutas conmutadas duplicadas sin considerar los efectos de latencia de los loops en la red.[2]

[2] http://aprenderedes.com/2006/11/protocolo-de-arbol-de-extensionstp/

2.1 PROTOCOLO STP

El STP (Spanning Tree Protocol) es un estándar utilizado en la administración de redes, basado en el algoritmo de Árbol, para describir como los switch pueden comunicarse para evitar loop o bucles en una red.

2.1.1 Configuracion Spanning Tree

A continuación se plantea un escenario de una red LAN empresarial en la que se poseen varios Switch dispuestos de la siguiente manera:

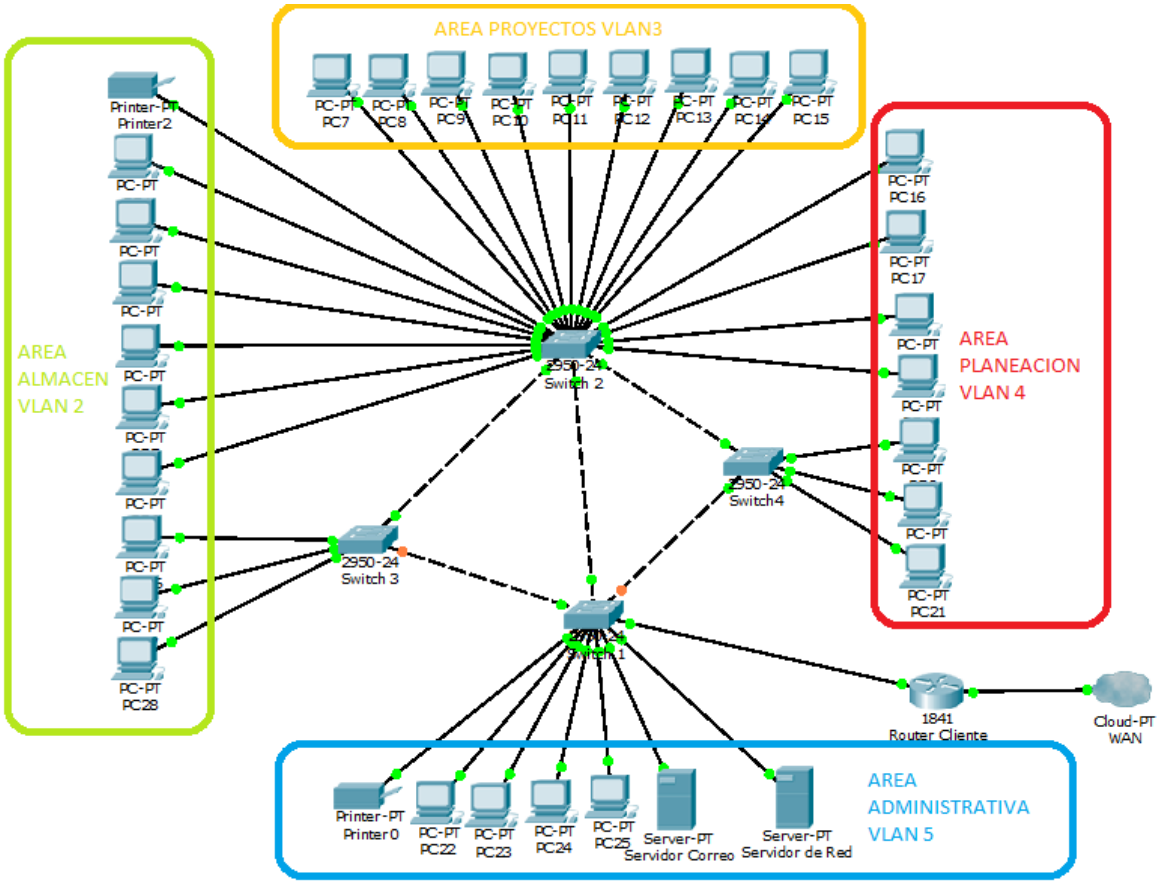

Figura 16. Escenario Spanning tree

Al tener varios puertos de comunicación entre los Switch, se crea redundancia entre los enlaces; lo cual es muy bueno debido a que si un enlace falla existen otros 2 para suplirlo; pero esta redundancia crea en las redes LAN empresariales los llamados bucles infinitos o Loop.

Para este problema existe un protocolo llamado **Spanning Tree (STP).** Normalmente los nuevos Switch por medio de la dirección MAC, determina cual es el Switch raíz y cuál es el designado, aunque normalmente por organización es mejor configurar manualmente un Switch como raíz.

Para que un Switch actué como raíz, se debe cambiar la prioridad, normalmente el valor por defecto de la prioridad es 32768, un valor más bajo hará que sea asignado como Raíz.

En el escenario se aprovechara que se poseen 5 Vlan diferentes; y colocaremos el Switch 1 como el Switch raíz de la Vlan 5 el Área Administrativa y la Vlan 1 de Gestión. El Switch 2 sera el switch raíz de las vlans 2, 3 y 4; las Areas: Almacén, Proyectos y Planeación.
Primero se iniciara configurando el tipo de modo de Spanning tree:

```
Switch_1(config)#spanning-tree mode ?
  pvst       Per-Vlan spanning tree mode
  rapid-pvst  Per-Vlan rapid spanning tree mode
```

PVST para el modo tradicional de Spanning tree y RAPID-PVST para el modo Rapid Spanning tree, lo importante es que todos los Switch trabajen en el mismo modo; para el escenario se trabajara con el Rapid- Spanning tree (RSTP) es una versión mejorada del spanning tree que es considerablemente más rápido convergiendo (recalculando la topología ante la caída de algún enlace).

Ahora continuaremos por hacer raíz de la Vlan 1 y la Vlan 5 al Switch 1:

```
Switch_1(config)#spanning-tree vlan 1,5 root primary
```

El comando anterior cambia la prioridad del Switch para las Vlan 1 y 5 de esa manera sea asignado como Switch Raiz.

Se realiza la configuración para que el Switch 2 sea el Switch Raiz de las Vlan 2, 3 y 4:

```
Switch_2(config)#spanning-tree vlan 2-4 root primary
```

La configuración que debe tener los 4 Switch es la siguiente:

```
Switch_1#show startup-config
Using 2259 bytes
!
version 12.1
no service password-encryption
!
hostname Switch_1
!
enable secret 5 $1$mERr$iofebau4guWgjL8ykTaad0
!
!
spanning-tree mode rapid-pvst          Modo de Rapid Spanning tree
spanning-tree portfast default         Hace mas rapido la deteccion de un loop o caida
spanning-tree vlan 1,5 priority 24576      Ser raiz para la vlan 1 y 5

Switch_2#show startup-config
Using 2712 bytes
!
version 12.1
no service password-encryption
!
hostname Switch_2
!
enable secret 5 $1$mERr$iofebau4guWgjL8ykTaad0
!
!
spanning-tree mode rapid-pvst
spanning-tree portfast default
spanning-tree vlan 2-4 priority 24576          Ser Switch Raiz para las vlans 2, 3 y 4

Switch_3#show startup-config
Using 1330 bytes
!
version 12.1
no service password-encryption
!
hostname Switch_3
!
enable secret 5 $1$mERr$iofebau4guWgjL8ykTaad0
!
```

```
!
spanning-tree mode rapid-pvst                Se configura que trabajen en RSTP
spanning-tree portfast default

Switch_4#show startup-config
Using 1331 bytes
version 12.1
no service password-encryption
!
hostname Switch_4
enable secret 5 $1$mERr$iofebau4guWgjL8ykTaad0
!
spanning-tree mode rapid-pvst                Se configura que trabajen en RSTP
spanning-tree portfast default
```

Solo se muestra la parte inicial de la configuración del Switch, debido a que el resto de la configuración de los Switch equivale a los puertos, con las interfaces troncalizadas para su interconexión y las Vlan asociadas a los puertos.

Con esto solucionaremos el problema de los bucles o Loop, que de existir en una red LAN empresarial hacen que esta colapse por la necesidad de retrasmisión y pérdida de paquetes.

Podemos realizar verificación de la configuración y funcionamiento del Spanning Tree en los switch con los siguientes comandos:

```
Switch_2#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0002 VLAN0003 VLAN0004
Extended system ID          is enabled
Portfast Default            is enabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default           is disabled
EtherChannel misconfig guard is disabled
UplinkFast                  is disabled
BackboneFast                is disabled
Configured Pathcost method used is short
```

```
Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
VLAN0001                  20        0        0        3         23
VLAN0002                  14        0        0        9         23
VLAN0003                  10        0        0       13         23
VLAN0004                  16        0        0        7         23
VLAN0005                  20        0        0        3         23
-------------------- -------- --------- -------- ---------- ----------
5 vlans                   80        0        0       35        115
```

Con el comando anterior podemos visualizar a cuales vlan el Switch es Raiz y verificar si se configuró correctamente.
Otro comando para la verificación del funcionamiento y configuración del Spanning tree es el siguiente:

```
Switch_2#show spanning-tree vlan 1
 Spanning tree enabled protocol rstp
 Root ID    Priority    24577
         Address     0060.3ED9.6785
         Cost        19
         Port        24(FastEthernet0/24)
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

 Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
         Address     0002.16A6.7D75
         Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
         Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/22           Desg FWD 19        128.22   P2p
Fa0/23           Desg FWD 19        128.23   P2p
Fa0/24           Root FWD 19        128.24   P2p
```

Con este comando podemos observar el funcionamiento de cada Vlan que queramos verificar, si se desea tener todas las Vlan se coloca el comando **show spanning-tree active.**

Con el comando **Show Spanning-tree Vlan 1**, se puede verificar el modo de protocolo de Spaning tree en el que se encuentra funcionando y las interfaces utilizadas para la interconexión entre Switch. En el ejemplo se observa, que para la Vlan 1 la interface Fa 0/24, es la conexión hacia el Switch Raíz de la Vlan 1.

Con esto habremos verificado el correcto funcionamiento del protocolo Spanning Tree, de esa manera se podrá tener redundandia en los enlaces sin los problemas de los loops.

3. PROTOCOLOS DE ENRUTAMIENTO

Existen dos modos de enrutamiento el estático y el dinámico.
Si este es estático se debe poder alcanzar desde el Router con un ping la dirección destino ejemplo.

IP route 0.0.0.0 0.0.0.0 10.1.1.2

Debe poderse alcanzar la IP 10.1.1.2 con un ping como se muestra en la prueba de ping que anterior, si hay más de una ruta estática se pueden verificar las direcciones destino de estas y deberían todas tener respuesta.
De no haber respuesta el problema es en el trayecto WAN.

Si el enrutamiento es dinámico el enrutamiento se puede verificar el funcionamiento de este con el comando **show ip route**, el cual nos muestra una tabla con las rutas que podemos alcanzar y la interface, también funciona para el enrutamiento estático.

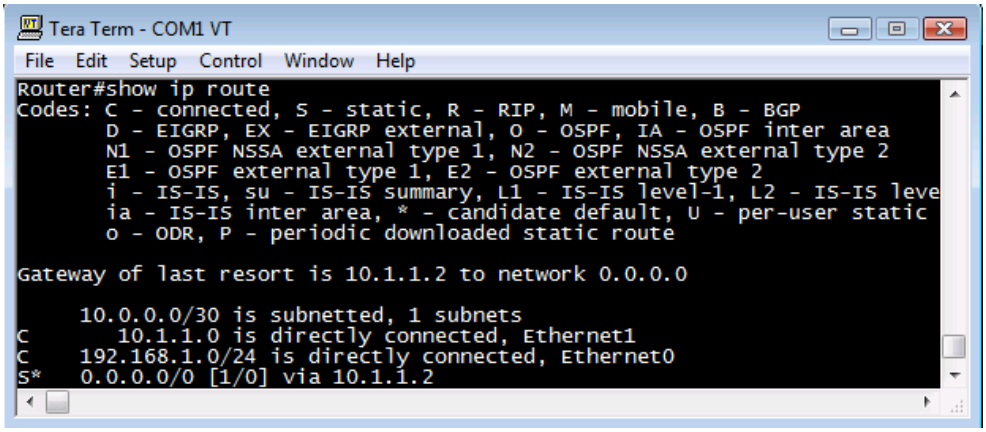

Figura 17. Comando Show ip route enrutamiento estático

En la figura 17, tenemos un ejemplo del comando **show ip route** podemos observar que en la parte superior la sigla que nos muestra por cual tipo de protocolo ha aprendido la ruta.

Podemos observar, que se tiene directamente conectada la red 10.1.1.0 en la Ethernet 1 y la red 192.168.1.0 en la Ethernet 0. También que existe uns ruta estática la cual enruta todo el trafico vía 10.1.1.2.

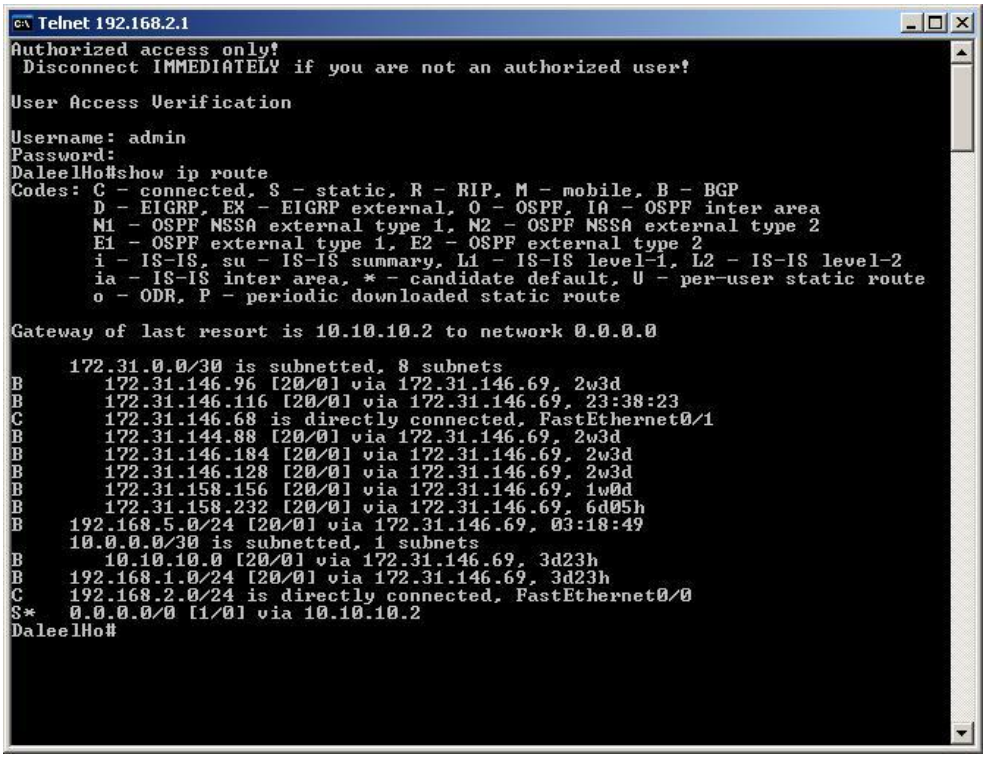

Figura 18. Comando show ip route enrutamiento dinámico

En la figura 18, es un ejemplo de una tabla de rutas aprendidas por medio de enrutamiento dinámico en este caso BGP, se conoce que se aprendieron por el protocolo BGP por la letra B al inicio de las rutas, esta letra nos muestra el tipo de enrutamiento utilizado.

Cuando en una red LAN empresarial, se posee más de una sede, se hace impráctico, difícil de administrar y configurar, el enrutamiento de manera estática; para esta problemática se crearon protocolos de enrutamiento dinámicos; los cuales se comunican entre sí para conocer las redes vecinas.

3.1 ENRUTAMIENTO DINAMICO

Los protocolos de enrutamiento dinámico son algoritmos que permiten decidir cuál es la mejor ruta que debe seguir un paquete para llegar a su destino.

Los protocolos que se explicarán corresponden a protocolos IGP, o protocolos de Gateway internos que son los utilizados en las redes LAN empresariales. Existen adicionalmente protocolos externos tales como BGP, pero estos son utilizados por

los proveedores de servicio y no por las empresas ya que su función no corresponde a enrutamientos de redes LAN.

3.1.1 RIP (Routing Information Protocol)

Es un protocolo universal de enrutamiento por vector de distancia que utiliza el número de saltos como único sistema métrico. Un salto es el paso de los paquetes de una red a otra. Si existen dos rutas posibles para alcanzar el mismo destino, RIP elegirá la ruta que presente un menor número de saltos. RIP no tiene en cuenta la velocidad ni la fiabilidad de las líneas a la hora de seleccionar la mejor ruta; esto es una gran desventaja debido a que puede que no asigne la mejor ruta para un destino. RIP envía un mensaje de actualización del enrutamiento cada 30 segundos (tiempo predeterminado en routers Cisco), en el que se incluye toda la tabla de enrutamiento del router, utilizando el protocolo UDP para el envío de los avisos. RIP está limitado a un número máximo de saltos de 15, con lo cual cualquier ruta con más de 15 saltos se considera inalcanzable; no soporta VLSM, y no soporta actualizaciones desencadenadas.

Para solucionar el problema de las redes de mascara variable, se creó la segunda versión de RIP (RIP-V2) este es un protocolo sin clase que admite CIDR, VLSM.

3.1.1.1 Configuración RIP:

```
Router# config terminal
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# network 172.16.0.0
Router(config-router)# version 2
```

3.1.2 IGRP (Interior Gateway Protocol).

Fue diseñado por Cisco a mediados de los ochenta, para corregir algunos de los defectos de RIP y para proporcionar un mejor soporte para redes grandes con enlaces de diferentes anchos de banda, siendo un protocolo propietario de Cisco. IGRP es un protocolo de enrutamiento por vector de distancia capaz de utilizar hasta 5 métricas distintas (ancho de banda K1, retraso K3, carga, fiabilidad, MTU), utilizándose por defecto únicamente el ancho de banda y el retraso. Estas métrica pueden referirse al ancho de banda, a la carga (cantidad de tráfico que ya gestiona un determinado router) y al coste de la comunicación (los paquetes se envían por la ruta más barata).

IGRP envía mensajes de actualización del enrutamiento a intervalos de tiempo mayores que RIP, utiliza un formato más eficiente, y soporta actualizaciones desencadenadas. IGRP posee un número máximo predeterminado de 100 saltos,

que puede ser configurado hasta 255 saltos, por lo que puede implementarse en grandes interconexiones donde RIP resultaría del todo ineficiente. IGRP puede mantener hasta un máximo de seis rutas paralelas de coste diferente; Por ejemplo, si una ruta es tres veces mejor que otra, se utilizará con una frecuencia tres veces mayor. IGRP no soporta VLSM. IGRP publica sus rutas sólo a los routers vecinos.

3.1.2.1 Configuracion IGRP

```
Router(config)#router igrp 100
Router(config-router)#network 192.168.1.0
Router(config-router)#network 200.200.1.0
```

router igrp 100 especifica a IGRP como protocolo de enrutamiento para el sistema autónomo 100, este valor varia de 1 a 65535

network, específica las redes directamente conectadas al router que serán anunciadas por IGRP

3.1.3 EIGRP (Enhaced IGRP).

Basado en IGRP y como mejora de este, es un protocolo híbrido que pretende ofrecer las ventajas de los protocolos por vector de distancia y las ventajas de los protocolos de estado de enlace. EIGRP soporta VLSM y soporta una convergencia muy rápida. EIGRP publica sus rutas sólo a los routers vecinos.

3.1.3.1 Configuración EIGRP:

```
router(config)#router eigrp 100
router(config-router)# network 192.168.16.0 0.0.0.255
router(config-router)#eigrp log-neighbor-changes
router(config-if)#bandwidth kilobits
```

Su configuración es idéntica a la de IGRP solo que este por aceptar VLSM utiliza la máscara Wilcard para determinar la subred a la que pertenece.

Bandwidth, el proceso de enrutamiento utiliza el comando bandwidth para calcular la métrica y es conveniente configurar el comando para que coincida con la velocidad, este comando se coloca en la interface.

log-neighbor-changes, habilita el registro de los cambios de adyacencia de vecinos para monitorear la estabilidad del sistema de enrutamiento y para ayudar a detectar problemas.

IGRP y EIGRP se redistribuyen automáticamente si ambos tienen el mismo número de sistema autonomo.

La desventaja de utilizar EIGRP es que es un protocolo propietario de Cisco, para lo cual se recomienda si la infraestructura de la empresa no tiene todos los equipos cisco; el siguiente protocolo.

3.1.4 OSPF (Open Short Path First)

Este es el protocolo más utilizado en Internet, es el protocolo recomendado de requerirse un protocolo de enrutamiento dinámico en las redes LAN empresariales; OSPF es un protocolo universal basado en el algoritmo de estado de enlace, desarrollado por el IETF para sustituir a RIP. Básicamente, OSPF utiliza un algoritmo que le permite calcular la distancia más corta entre la fuente y el destino al determinar la ruta para un grupo específico de paquetes. OSPF soporta VLSM, ofrece convergencia rápida, autenticación de origen de ruta, y publicación de ruta mediante multidifusión.

OSPF publica sus rutas a todos los routers del mismo área. Funciona dividiendo una intranet o un sistema autónomo en unidades jerárquicas de menor tamaño. Cada una de estas áreas se enlaza con un área backbone mediante un router fronterizo. Así, todos los paquetes direccionados desde un área a otra diferente, atraviesan el área backbone. OSPF envía Publiciones del Estado de Enlace (Link-State Advertisement – LSA) a todos los routers pertenecientes a la misma área jerárquica mediante multidifusión IP.

Los routers vecinos intercambian mensajes Hello para determinar qué otros routers existen en una determinada interfaz y sirven como mensajes de actividad que indican la accesibilidad de dichos routers. Cuando se detecta un router vecino, se intercambia información de topología OSPF. La información de la LSA se transporta en paquetes mediante la capa de transporte OSPF (con acuse de recibo) para garantizar que la información se distribuye adecuadamente. [3]

[3] http://www.guillesql.es/Articulos/Manual_Cisco_CCNA_Protocolos_Enrutamiento.aspx

Para la configuración de OSPF se requiere un número de proceso, ya que se pueden ejecutar distintos procesos OSPF en el mismo routers. Los administradores acostumbran usar un número de SA como número de proceso

3.1.4.1 Configuración OSPF

Router(config)#router ospf 1
Router(config-router)#log-adjacency-changes
Router(config-router)#network 10.1.4.0 0.0.0.255 area 0
Router(config-router)#network 192.168.1.0 0.0.0.7 area 0

Al igual que IGRP y EIGRP, utiliza sistemas Autónomos que van desde 1 a 65535. Además se agrega en la parte de Network el área a la que pertenece la red con esto se pueden crear diferentes áreas para el manejo jerárquico de las redes de la empresa.

3.1.5 Comparación Protocolos dinámicos

En la siguiente tabla podemos tener una comparación de las características de cada protocolo.

Caracteristicas	RIP	OSPF	IGRP	EIGRP
Tipo	Vector – Distancia	Estado enlace	Vector – Distancia	Vector - Distancia
Tiempo de convergencia	Lento	Rápido	Lento	Rápido
Soporta VLSM	No	Si	No	Si
Consumo de Ancho de Banda	Alto	Bajo	Alto	Bajo
Consumo de recursos	Bajo	Alto	Bajo	Bajo
Mejor escalamiento	No	Si	Si	Si
De libre uso o propietario	Libre uso	Libre uso	Propietario	Propietario

Tabla 1. Comparación protocolos dinámicos

4. EJEMPLOS CONFIGURACION SWITCHES Y ROUTERS

A continuación mostraremos algunos escenarios de ejemplos de configuraciones de switch y routers en las soluciones de problemas en las redes LAN empresariales.
Se ha planteado diferentes escenarios para mostrar los problemas más comunes.

En una empresa lo más posible es encontrarnos con un escenario parecido al siguiente:

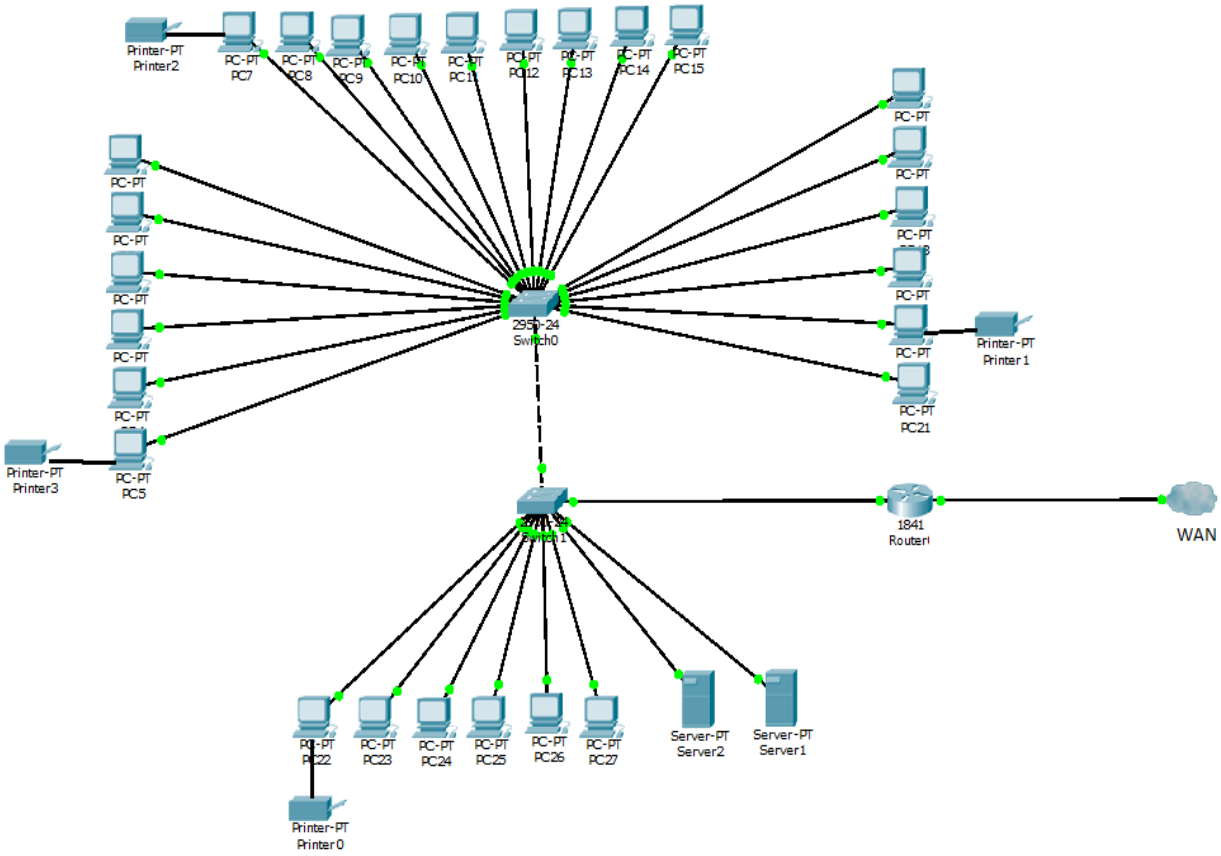

Figura 19. Escenario red LAN empresarial

Donde se encuentra un Router que nos conecta a la red WAN con el proveedor de servicio y un Switch o varios dependiendo del caso, que interconectan los equipos de la empresa.

En la actualidad es muy raro que las empresas aun utilicen HUB; de haber alguno, lo primero que se debe hacer es su inmediato cambio a un Switch, debido a que el

HUB simplemente es un repetidor el cual genera tráfico innecesario, generando colisiones y por consiguiente lentitud de la red LAN.

En el escenario planteado se puede observar como todos los equipos van conectados a dos Switch, normalmente encontraremos en una red LAN empresarial, una sola red para todos los equipos; la cual muy seguramente será dada por DHCP por medio de un servidor.

Esta configuración de red trae consigo muchos problemas, normalmente informados por la empresa como lentitud en la red, hasta para comunicación interna entre equipos; esto es debido a que no hay una correcta organización de la red y hace que todo sea compartido generando colisiones y desaprovechamiento de los recursos.

El utilizar DHCP facilita la configuración inicial de la red debido a que cada equipo toma su dirección de un pool de direcciones (grupo de direcciones IP) automáticamente, pero esto dificulta el determinar un problema en la red debido a que no conocemos con exactitud que IP posee cada usuario.

Se recomienda el direccionamiento estático el cual debe ser configurado en cada equipo y asignar una tabla donde se conoce a que usuario o funcionario corresponde cada IP. Con esto es fácil determinar los equipos con problemas en la red LAN empresarial.

4.1 CONFIGURACIÓN VLAN

Para realizar una mejor organización y aprovechamiento de los recursos de la red, se debe realizar es un estudio del funcionamiento de la empresa, normalmente las empresas se encuentran divididas en departamentos o áreas las cuales poseen diferentes funciones, eso mismo se debe realizar en una red LAN empresarial dividiéndola en áreas o departamentos por medio de redes virtuales (VLANS).
De esta manera tendremos mejor organizada nuestra red LAN empresarial.

Como podemos observar en la figura 20, se divide la empresa en diferentes departamentos con vlan diferentes.

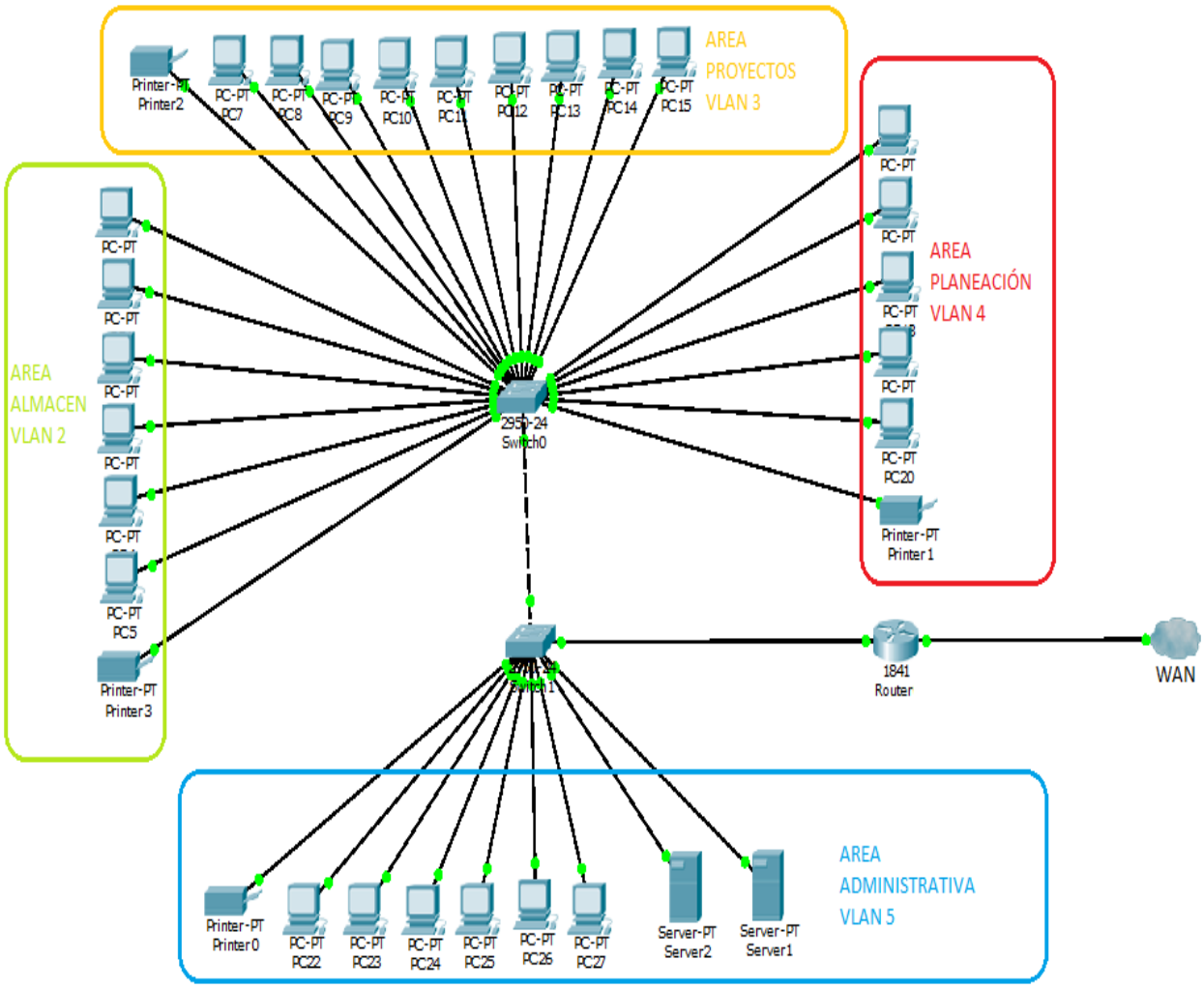

Figura 20. Escenario red LAN empresarial VLAN

Se crearán Vlan para cada departamento de ser necesario; o departamentos que tengan una comunicación continua entre sí; se creara una sola Vlan en la cual se encontrarán estos 2 departamentos.

En el escenario planteado como ejemplo, se realiza la división de la red empresarial en 5 Vlan, las cuales son:

- **VLAN 1:** Se deja para gestionar y administrar los equipos de manera remota, los equipos a gestionar son los Switch y el Router.
- **VLAN 2:** Se crea para el área de Almacén, en el cual se realizan las compras e inventario de los elementos de la empresa.
- **VLAN 3:** Se crea para el área de Proyectos y desarrollo.

- **VLAN 4:** Se crea para el área de Planeación.
- **VLAN 5:** Se crea para el área administrativa donde se encuentran los servidores, la gerencia, contabilidad y atención al cliente.

Al dividir la red empresarial en diferentes Vlan, al generarse un problema en un equipo de la red LAN, este problema solo afectaran el Sector o Vlan en que se encuentre.

Normalmente se dividen las Vlan partiendo de la organización de la empresa, debido a que es más común el tráfico entre los equipos del área de trabajo que entre departamentos.

De todas maneras es importante la configuración y utilización de un Router. Por medio de este podemos interconectar las Vlan para de esa manera no queden totalmente aisladas las diferentes áreas o departamentos de una empresa.

Para la creación de Vlan se requiere la creación de un direccionamiento organizado, debido a que cada Vlan tendrá diferente direccionamiento de red.
De esa manera las redes serán las siguientes:

- VLAN 1 Gestion: red IP 192.168.0.0
- VLAN 2 Almacen: red IP 192.168.1.0
- VLAN 3 Proyectos: red IP 192.168.2.0
- VLAN 4 Planeación: red IP 192.168.3.0
- VLAN 5 Administrativa: red IP 192.168.4.0

Como se observa en el escenario planteado en la figura 21, se configura de manera estática los PC con las direcciones que corresponden a cada una de las 5 Vlan creadas, de esta manera creamos independencia de red y de recursos entre los diferentes departamentos de la empresa.

Para el correcto funcionamiento de este escenario se realizará la configuración de los dos Switch y el Router.

El proceso de configuración de los Switch y el Router se iniciara desde el más alejado al Router, el cual en el escenario se llamo Switch_2.

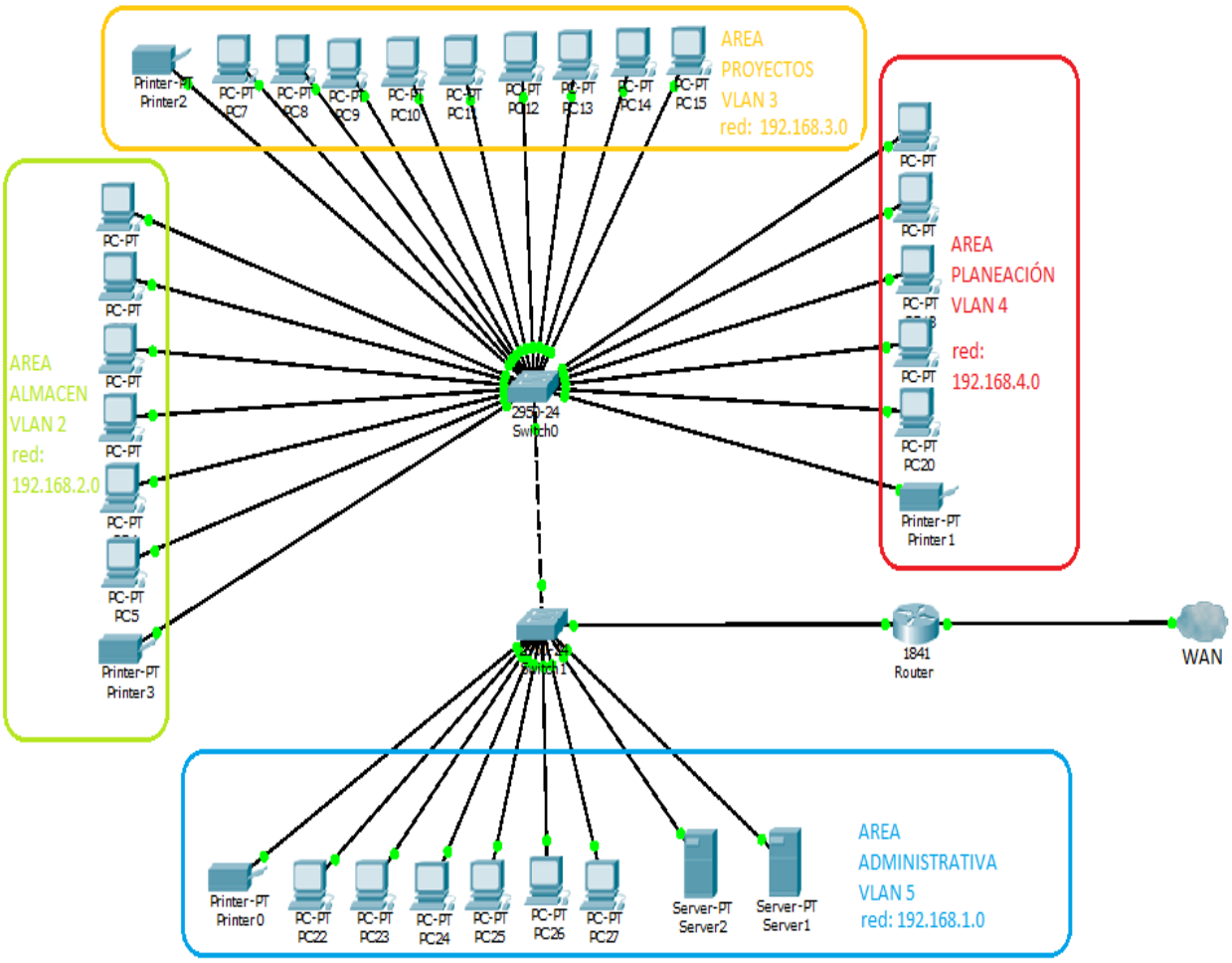

Figura 21. Escenario red LAN con 5 Vlan

Lo primero que se debe realizar es crear las Vlan en el Switch 2. La configuración se realiza de la siguiente manera:

Switch_2#vlan database **Se ingresa para crear las vlans en el switch**
% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.

Switch_2(vlan)#vlan 2 **se coloca la vlan 2 y el switch la agrega**
VLAN 2 added:
Name: VLAN0002
Switch_2(vlan)#vlan 3 **Se realize igualmente con cuantas vlans necesitemos**
VLAN 3 added:
Name: VLAN0003

```
Switch_2(vlan)#vlan 4
VLAN 4 added:
    Name: VLAN0004
Switch_2(vlan)#vlan 5
VLAN 5 added:
    Name: VLAN0005
Switch_2(vlan)#exit
APPLY completed.
Exiting....
```

Con esto crearemos las 5 Vlan que se utilizan en la red LAN empresarial, según el esquema que hemos planteado. Es importante crear todas las Vlan, debido a que se realizara enlaces troncales para intercomunicarnos con el Router y entre los dos Switch, de esta manera todas las Vlans podrán comunicarse entre sí de ser necesario.

Ahora se requiere asignar los puertos del Switch a cada Vlan, para esto hay que tener cuidado de que el puerto asignado a la Vlan corresponda al área que se desea asignar.

Esta es la configuración del Switch 2 en el escenario planteado. En color rojo se explican los comandos colocados en la configuración del switch 2:

```
Switch_2#show startup-config
Using 2613 bytes
version 12.1
no service password-encryption
!
hostname Switch_2                    Se coloca el nombre que tendra el switch
!
enable secret 5 $1$mERr$iofebau4guWgjL8ykTaad0   pass de ingreso al modo privilegiado en el
!                                                escenario planteado es "cliente"
interface FastEthernet0/1
 description --- VLAN AREA ALMACEN ---     muy importante para visualizar el puerto y
 switchport access vlan 2                  área se asigna la vlan 2 al Puerto f 0/1
!
interface FastEthernet0/2
 description --- VLAN AREA ALMACEN ---
 switchport access vlan 2                  Se asiganan todos los puertos que
```

```
!
interface FastEthernet0/3
 description --- VLAN AREA ALMACEN ---
 switchport access vlan 2
!
interface FastEthernet0/4
 description --- VLAN AREA ALMACEN ---
 switchport access vlan 2
!
interface FastEthernet0/5
 description --- VLAN AREA ALMACEN ---
 switchport access vlan 2
!
interface FastEthernet0/6
 description --- VLAN AREA ALMACEN ---
 switchport access vlan 2
!
interface FastEthernet0/7
 description --- VLAN AREA ALMACEN ---
 switchport access vlan 2
!
interface FastEthernet0/8
 description --- VLAN AREA PROYECTOS ---
 switchport access vlan 3
!
interface FastEthernet0/9
 description --- VLAN AREA PROYECTOS ---
 switchport access vlan 3
!
interface FastEthernet0/10
 description --- VLAN AREA PROYECTOS ---
 switchport access vlan 3
!
interface FastEthernet0/11
 description --- VLAN AREA PROYECTOS ---
 switchport access vlan 3
!
interface FastEthernet0/12
 description --- VLAN AREA PROYECTOS ---
 switchport access vlan 3
```

corresponde a la vlan 2 de ALMACEN

Se coloca el nombre del area al que pertenece
Al igual a la vlan 2 se asigana la vlan 3 a cada puerto que corresponda al area PROYECTOS

```
!
interface FastEthernet0/13
 description --- VLAN AREA PROYECTOS ---
 switchport access vlan 3
!
interface FastEthernet0/14
 description --- VLAN AREA PROYECTOS ---
 switchport access vlan 3
!
interface FastEthernet0/15
 description --- VLAN AREA PROYECTOS ---
 switchport access vlan 3
!
interface FastEthernet0/16
 description --- VLAN AREA PROYECTOS ---
 switchport access vlan 3
!
interface FastEthernet0/17
 description --- VLAN AREA PROYECTOS ---
 switchport access vlan 3
!
interface FastEthernet0/18
 description --- VLAN AREA PLANEACION ---
 switchport access vlan 4
!
interface FastEthernet0/19
 description --- VLAN AREA PLANEACION ---
 switchport access vlan 4
!
interface FastEthernet0/20
 description --- VLAN AREA PLANEACION ---
 switchport access vlan 4
!
interface FastEthernet0/21
 description --- VLAN AREA PLANEACION ---
 switchport access vlan 4
!
interface FastEthernet0/22
 description --- VLAN AREA PLANEACION ---
 switchport access vlan 4
```

Se coloca igualmente al area
Se asigna la vlan 4 para el area de PLANEACION

```
!
interface FastEthernet0/23
 description --- VLAN AREA PLANEACION ---
 switchport access vlan 4
!
interface FastEthernet0/24
 description --- ENLACE TRONCAL SWITCH_1 ---La conexion con el otro switch debe ser
 switchport mode trunk                      troncal por el enlace va el trafico de la s
!                                           vlans hacia el switch 1.
interface Vlan1
 description --- VLAN GESTION ---       Se deja la Vlan 1 para la gestión remota del switch
 ip address 192.168.10.3 255.255.255.0      se asigna una dirección IP dentro de la red
!                                           de la Vlan1
ip default-gateway 192.168.10.1         Se configure el gateway hacia la dirección del
!                                       router
line con 0
!
line vty 0 4                            Línea de comandos para el ingreso remoto
 password enter                         Se asigna pass de ingreso como enter para telnet
 login
line vty 5 15
 login
end
```

Al finalizar la configuración del Switch 2, se puede verificar que los puertos quedaron asignados a las Vlan correspondientes por medio del comando:

```
Switch_2#show vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
2    VLAN0002                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7
3    VLAN0003                          active    Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17
4    VLAN0004                          active    Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23
5    VLAN0005                          active
1002 fddi-default                      active
```

1003 token-ring-default active

Se puede observar la distribución de los puertos a cada Vlan creada en el switch2. Con este comando se verifica, que todas las conexiones del Switch2 se encuentren correctamente; que los puertos asignados correspondan a la conexión con los equipos en la red LAN.

Con esto hemos finalizado la configuración del Switch2, se han creado exitosamente las cinco (5) Vlan de las áreas de **ALMACEN, PROYECTOS, PLANEACION, ADMINISTRATIVA** y la Vlan de **GESTION** de los equipos.
Por ahora solo se tiene comunicación entre los equipos de una misma Vlan.

Se continuara con la configuración del Switch 1, al cual se le crearan igualmente todas las Vlan, debido a que por el puerto de interconexión entre los dos Switch, de manera troncalizada pasara la información de todas las Vlan hacia el Router.
Se realiza la misma operación de creación de las Vlan del Switch 2 en el Switch 1.

Finalizada la creación de las 5 Vlan, se procede a la configuración del Switch 1 la cual es la siguiente:

```
Switch_1#show startup-config
Using 2024 bytes
!
version 12.1
no service password-encryption
!
hostname Switch_1                          Se configura el nombre del switch 1
!
enable secret 5 $1$mERr$iofebau4guWgjL8ykTaad0   se coloca pass de enable como “cliente”
!
!
!
interface FastEthernet0/1
 description --- ENLACE TRONCAL CON SWITCH_2 ---   Conexion con el switch 2 el cual se
 switchport mode trunk                             debe configurar como troncalizado
!
interface FastEthernet0/2
 description --- VLAN AREA ADMINISTRATIVA ---      Puerto designado  a Area ADMIN
 switchport access vlan 5                          Se asigna la Vlan 5 al puerto
!
```

```
interface FastEthernet0/3
 description --- VLAN AREA ADMINISTRATIVA ---
 switchport access vlan 5
!
interface FastEthernet0/4
 description --- VLAN AREA ADMINISTRATIVA ---
 switchport access vlan 5
!
interface FastEthernet0/5
 description --- VLAN AREA ADMINISTRATIVA ---
 switchport access vlan 5
!
interface FastEthernet0/6
 description --- VLAN AREA ADMINISTRATIVA ---
 switchport access vlan 5
!
interface FastEthernet0/7
 description --- VLAN AREA ADMINISTRATIVA ---
 switchport access vlan 5
!
interface FastEthernet0/8
 description --- VLAN AREA ADMINISTRATIVA ---
 switchport access vlan 5
!
interface FastEthernet0/9
 description --- VLAN AREA ADMINISTRATIVA ---
 switchport access vlan 5
!
interface FastEthernet0/10
 description --- VLAN AREA ADMINISTRATIVA ---
 switchport access vlan 5
!
interface FastEthernet0/11
 description --- VLAN AREA ADMINISTRATIVA ---
 switchport access vlan 5
!
interface FastEthernet0/12
 description --- VLAN AREA ADMINISTRATIVA ---
 switchport access vlan 5
!
```

Se asigna cada Puerto que pertenesca Area ADMINISTRATIVA

```
interface FastEthernet0/13
 description --- VLAN AREA ADMINISTRATIVA ---
 switchport access vlan 5
!
interface FastEthernet0/14
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24              puerto desiganado al enlace troncal con el Router
 description --- ENLACE TRONCAL A ROUTER_CLIENTE ---
 switchport mode trunk                  Se configure como troncal
!
interface Vlan1
 description --- VLAN GESTION ---       Se asigna la vlan para gestión remota del equipo
 ip address 192.168.10.2 255.255.255.0  por medio de Telnet el cual puede realizar gestión
!                                       Desde cualquier equipo de la red LAN empresarial
ip default-gateway 192.168.10.1
!
line con 0
!
line vty 0 4
 password enter                         Se asigna un pass para poder realizar telnet
 login
line vty 5 15
 login
!
!
End
```

En este Switch (Switch_1) se encuentran 2 enlaces troncales. El primero que viene del Switch 2 y el segundo que se comunica con el Router. Es muy importante colocarlos en modo troncalizado, de no ser así no habría comunicación ni con el Router ni con el Switch 2.

Se denomina troncalizado, porque por medio de él viajan las 5 Vlan de manera independiente. Es como si el enlace lo dividieran en 5 caminos, uno para cada Vlan.

Con esto ya se tienen configurados los 2 Switches del escenario planteado de la red LAN empresarial.

Ahora solo nos falta la configuración del Router, este nos permitirá la interconexión entre las Vlan.
A este proceso se le conoce como VTP (protocolo de enlace troncal).

La siguiente es la configuración que debería tener el Router en el escenario planteado, el Router lo llamaremos Router_Cliente:

```
ROUTER_CLIENTE#show star
Using 1459 bytes
!
version 12.4
no service password-encryption
!
hostname ROUTER_CLIENTE     Al igual que al switch se configure el nombre del equipo
!
!
enable secret 5 $1$mERr$iofebau4guWgjL8ykTaad0     se utiliza mismo pass “cliente”
!
ip ssh version 1
!
interface FastEthernet0/0                          Puerto designado para la LAN del cliente
 description --- LAN CLIENTE ---
 no ip address                                     no se coloca IP porque se trabaja
troncalizado
 duplex auto                                       por las 5 vlans
 speed auto
```

```
!
interface FastEthernet0/0.1                    creación subinterface para la vlan 1
 description --- GESTION ---                   vlan 1 sera la vlan de gestión de los equipos
 encapsulation dot1Q 1 native                  se coloca tipo de encap IEEE 802.1Q
 ip address 192.168.10.1 255.255.255.0         se asigna la primera ip del rango
!
interface FastEthernet0/0.2                    Subinterface para la vlan 2
 description --- LAN AREA ALMACEN ---          Vlan asignada al area ALMACEN
 encapsulation dot1Q 2                         tipo de encap y asignación a la vlan 2
 ip address 192.168.2.1 255.255.255.0          Configura la primera ip del rango como el
!                                              gateway en los PC de la vlan 2
interface FastEthernet0/0.3
 description --- LAN AREA PROYECTOS ---
 encapsulation dot1Q 3
 ip address 192.168.3.1 255.255.255.0
!
interface FastEthernet0/0.4                    se realiza igual cada subinterface acorde
 description --- LAN AREA PLANEACION ---       al numero de vlan asociada con la
 encapsulation dot1Q 4                         encapsulación y la dirección IP del rango
 ip address 192.168.4.1 255.255.255.0          correspondiente a cada vlan
!
interface FastEthernet0/0.5
 description --- LAN AREA ADMINISTRATIVA ---
 encapsulation dot1Q 5
 ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/1
 description --- WAN ---                                interface de conexion wan
 ip address 10.1.1.2 255.255.255.252                    direccion ip de la wan
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 192.168.2.0 255.255.255.0 FastEthernet0/0.2     Se configure rutas estaticas
ip route 192.168.3.0 255.255.255.0 FastEthernet0/0.3     para cada vlan
ip route 192.168.4.0 255.255.255.0 FastEthernet0/0.4
```

```
ip route 192.168.1.0 255.255.255.0 FastEthernet0/0.5
ip route 192.168.10.0 255.255.255.0 FastEthernet0/0.1
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1        se configure ruta por defecto hacia la wan
!
line con 0
line vty 0 4                                    configura pass para ingreso por telnet
 password enter
 login
End
```

Como se observa en la configuración del Router, se debe crear una subinterface para cada Vlan; en la interface que va conectada a la LAN, en el escenario la interface f 0/0.

Cada subinterface debe tener el mismo número de Vlan, de la siguiente manera:

- Vlan 1 Subinterface fastethernet 0/0.1
- Vlan 2 Subinterface fastethernet 0/0.2
- Vlan 3 Subinterface fastethernet 0/0.3
- Vlan 4 Subinterface fastethernet 0/0.4
- Vlan 5 Subinterface fastethernet 0/0.5

Igualmente en la encapsulación debe colocarse **encapsulation dot1Q** #, el numero al cual pertenece la Vlan. Con estos parámetros correctamente configurados tendremos conexión entre las 5 Vlan y el Router.
Se agregan rutas estáticas para la comunicación entre Vlan y una ruta por defecto para que todo el tráfico diferente a la red empresarial salga hacia la WAN.

Con estos cambios se habrá mejorado la red LAN empresarial, organizándola de manera que sea de más fácil administración, detección de errores y problemas. Lo más importante es que la red es mucho más eficiente, lo cual se observara en los usuarios como una red LAN que opera más rápido, con estos cambios mejora considerablemente la interconexión entre equipos LAN.

4.2 Configuración OSPF

Para continuar con los mejoramientos de una red LAN empresarial, continuaremos con el estudio del enrutamiento entre sedes empresariales; en los escenarios

planteados anteriormente se habían creado una ruta estática por defecto, debido a que la red LAN empresaria correspondía a una sola sede.
Pero en el caso de cuando se posee más de una sede, se hace impráctico y de muy difícil administrar y configurar, el enrutamiento de manera estática; para esta problemática se crearon protocolos de enrutamiento, en el escenario planteado se explicara la configuración por medio de OSPF que es el protocolo recomendado actualmente.

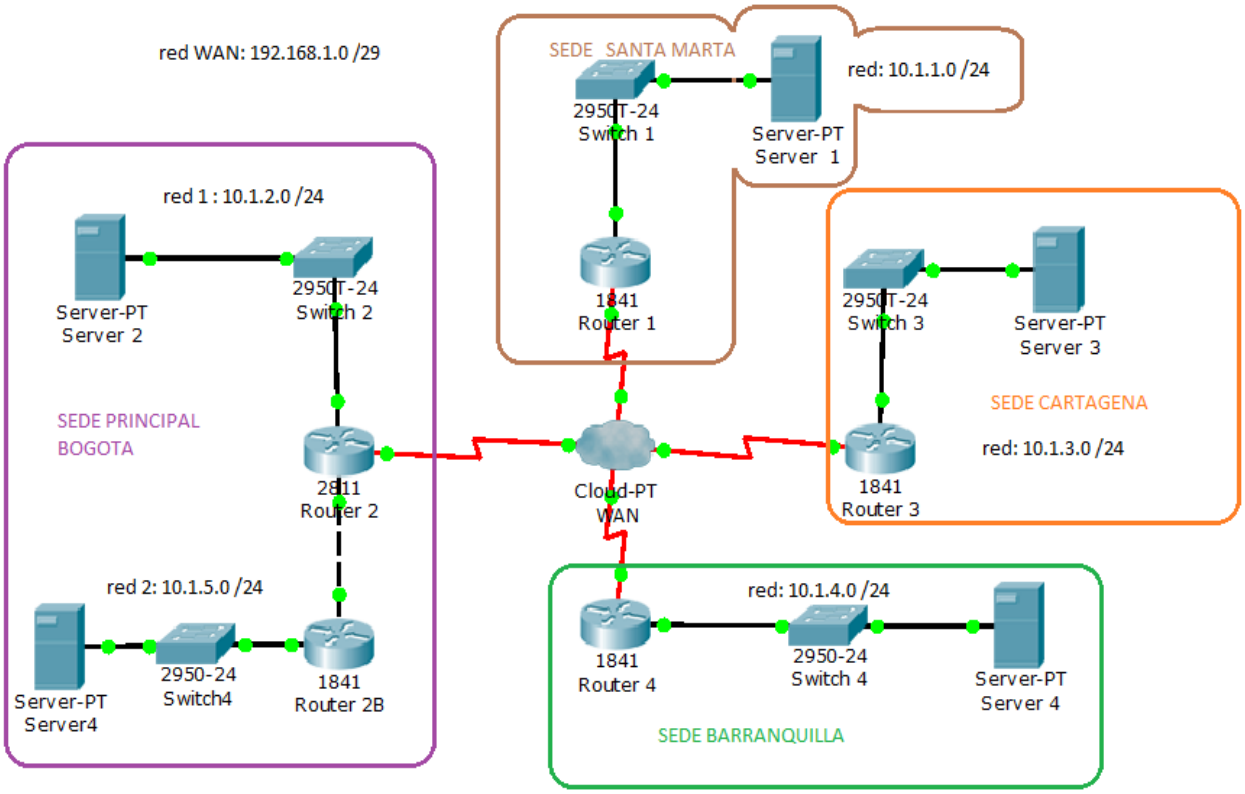

Figura 22. Escenario enrutamiento OSPF

En el escenario nos hemos planteado 4 sedes en las ciudades Bogotá, Cartagena, Barranquilla y Santa Marta.

Para la configuración del enrutamiento, es importante tener claro el direccionamiento que posee cada sede, debido a que la unión de todas las redes independientes por sede, vendría a ser una única red; la red LAN empresarial. Por esta razón no pueden existir redes iguales o duplicados de IP.

Se recomienda la utilización del protocolo de enrutamiento OSPF, debido a que es más rápido para converger después de algún cambio de la red, es escalable, con lo cual la red empresarial puede crecer y crecer sin ningún inconveniente.

Para el enrutamiento OSPF es necesario configurar las redes que tiene cada Router conectadas directamente. En el Router 3 la sede de Cartagena, en OSPF se configura la red LAN 10.1.3.0 con mascara 255.255.255.0 y la red WAN 192.168.1.0 con mascara 255.255.255.248.

A continuación se mostrara la configuración del OSPF en cada Router del escenario:

Router 1 sede Santa Marta:

```
router ospf 1
 log-adjacency-changes
 redistribute connected subnets
 network 10.1.1.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.7 area 0
```

Router 2 Sede Principal Bogota:

```
router ospf 1
 log-adjacency-changes
 network 10.1.2.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.7 area 0
 network 192.168.2.0 0.0.0.3 area 0
```

Router 2B Sede Bogota:

```
router ospf 1
 log-adjacency-changes
 network 10.1.5.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.3 area 0
```

Router 3 Sede Cartagena:

```
router ospf 1
 log-adjacency-changes
```

redistribute connected subnets
network 10.1.3.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.7 area 0

Router 4 Sede Barranquilla:

router ospf 1
log-adjacency-changes
network 10.1.4.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.7 area 0

Como se puede observar en cada uno de los Router, se configuran las redes directamente conectadas. Es importante que todas tengan el mismo número de proceso de OSPF, en el escenario se coloco el numero 1; pero puede ser cualquier valor entre 1 y 65.535.

Se pueden configurar diferentes áreas, debido a que es una sola red empresarial se coloca toda como area 0 (si se utiliza una sola área debe ser el área 0).

Para la verificación del funcionamiento del protocolo de enrutamiento OSPF se coloca el siguiente comando:

Router_3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
*** - candidate default, U - per-user static route, o - ODR**
P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 5 subnets
O 10.1.1.0 [110/782] via 192.168.1.1, 00:38:33, Serial0/0/0 **Las mostradas como O son**
O 10.1.2.0 [110/782] via 192.168.1.2, 00:38:53, Serial0/0/0 **rutas conocidas por OSPF**
C 10.1.3.0 is directly connected, FastEthernet0/0 **red conectada directamente**
O 10.1.4.0 [110/782] via 192.168.1.4, 00:38:53, Serial0/0/0
O 10.1.5.0 [110/783] via 192.168.1.2, 00:08:38, Serial0/0/0

```
    192.168.1.0/29 is subnetted, 1 subnets
C      192.168.1.0 is directly connected, Serial0/0/0
    192.168.2.0/30 is subnetted, 1 subnets
O      192.168.2.0 [110/782] via 192.168.1.2, 00:38:53, Serial0/0/0
```

Con el comando **Show ip route**, podemos verificar que el Router si está aprendiendo las rutas por medio de OSPF, y que se encuentra correctamente configurado y está funcionando correctamente.

Otro comando que nos puede servir para verificar el protocolo de enrutamiento es **show ip protocol**, este comando nos muestra el protocolo que se encuentra activo en el Router:

```
Router_3#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.1.3
Redistributing External Routes from,
    connected
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.1.3.0 0.0.0.255 area 0
    192.168.1.0 0.0.0.7 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.1.4          110      00:18:37
    192.168.1.1          110      00:50:00
    192.168.1.2          110      00:18:39
  Distance: (default is 110)
```

Con el comando anterior podemos verificar que el protocolo de enrutamiento es el **ospf 1** y las redes configuradas en OSPF.
Con el correcto funcionamiento del protocolo de enrutamiento OSPF tendremos conexión entre todas las sedes de la red LAN empresarial.

4.3 Aplicación NAT

Como ya sabemos prácticamente toda red LAN empresarial requiere tener acceso al Internet por tal razón requiere de dirección IP pública para hacerlo.
Debido a que las direcciones públicas son pagas, las empresas no utilizarían una dirección IP pública para cada equipo de la red LAN, para solucionar esto se implementa una técnica llamada **NAT** (Network Address Translation), que permite conectar varios PCs de una misma subred a Internet, utilizando únicamente una dirección IP pública para ello.

Como sólo queremos utilizar una dirección pública, ésta se asigna al equipo que implementa NAT (normalmente es un Router), mientras que los ordenadores de la subred poseen direcciones privadas estas últimas sólo son válidas para identificar al ordenador en el ámbito de la subred.

Esto se consigue sustituyendo cada dirección origen privada de las cabeceras de los paquetes IP por la dirección pública, por lo tanto todos los paquetes de salida tendrán la misma dirección origen.

Para poder identificar entonces cada tráfico de los diferentes ordenadores, se utiliza el número de puerto de cada conexión.

Para hacer todo esto, el Router debe mantener una tabla con la dirección y puerto real de la máquina, el número de puerto que se le ha asignado, y dirección y puerto destino. De esta forma el Router puede entregar los paquetes de vuelta a los ordenadores correspondientes. Resumiendo, los paquetes de vuelta contendrán todos la misma dirección destino, pero con diferente número de puerto que será lo que identifique a cada conexión y el Router sepa así a quién mandarlo.

Con esta Técnica también se genera seguridad en la red LAN empresarial debido a que solo el Router donde se implementa el NAT conoce la dirección exacta de cada máquina en la LAN y no se publica en Internet.[4]

4.3.1 Configuración NAT

Para realizar la configuración de NAT en un Router, se ha planteado el siguiente escenario de una red LAN empresarial, figura 23.

[4] http://www.t2app.com/util-ip/nat.htm

En ella la red LAN empresarial posee un direccionamiento privado con la red 10.1.1.0, y para salir a Internet todos sus equipos se implementa NAT en el Router con la dirección Pública 190.144.2.22.

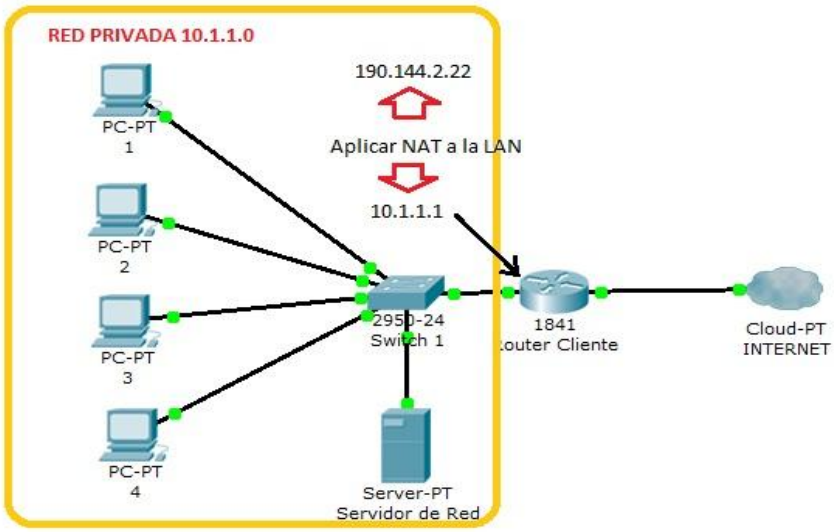

Figura 23. Escenario NAT

La configuración que se realizaría en el router para la implementación del NAT es la siguiente:

```
Router_Cliente#show run
Building configuration...
version 12.4
no service password-encryption
!
hostname Router_Cliente
!
!
ip ssh version 1
!
!
interface Loopback10
 description --- DIRECCION PUBLICA ---
 ip address 190.144.2.22 255.255.255.252
!
```

Se crea interface con la direccion publica para asociarla luego a la red LAN en la interface F0/0 donde se conecta al Switch

```
interface FastEthernet0/0
 description --- LAN CLIENTE ---
 ip address 10.1.1.1 255.255.255.0
 ip nat inside                                  Comando para informar que corresponde
 duplex auto                                    a la interface con los datos de entrada
speed auto
!
interface FastEthernet0/1
 description --- WAN PROVEEDOR ---
 ip address 10.168.1.1 255.255.255.252
 ip nat outside                                 Comando para informar interface de
 duplex auto                                    salida de la informacion
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip nat inside source list 101 interface Loopback10 overload    Aplicacion del NAT donde se
ip classless                                                   toma toda la red LAN de la access
ip route 0.0.0.0 0.0.0.0 10.168.1.2                            list 101 y se aplica la direccion pub
!                                                              en la loopback10.
!
access-list 101 permit ip 10.1.1.0 0.0.0.255 anylista para agregar toda la red LAN a
!                                              la direccion publica, se pueden
line con 0                                     asignar varias redes sobre la misma
line aux 0                                     lista de acceso
line vty 0 4
!
!
End
```

Con esta configuración cuando un equipo de la red requiera salir a Internet saldrá por la dirección IP pública y la traducción será realizada por el Router.
Esta configuración nos permites aislar nuestros equipos finales del Internet para evitar sean blancos de ataque, lo cual genera seguridad y optimización de los recursos de red.

4.4 CONFIGURACION Calidad de Servicio (QoS)

Existe diferentes métodos más avanzados de mejoramiento en las comunicaciones de una empresa como son la aplicación de calidad de servicio o QoS, lo importante al tener en cuenta es que al aplicar estos métodos se requiere que se aplique a todos los equipos involucrados, sean switch o routers en todo el trayecto, de no ser asi no tendría ninguna función.

En resumen la QoS funciona etiquetando prioridades de paquetes; ejemplo la voz se prioriza para que no tenga retardo antes que los datos debido a que esta se requiere sea en tiempo real.

Existen diferentes métodos de aplicación de QoS pero lo más utilizado es configurar prioridad en los equipos entre más alto es este número, mayor será la prioridad y más rápido se realizará el envío de esa información marcada con esa prioridad en otras palabras menor retardo y tiempo de espera.

Esto es muy importante porque de esa manera no habrá competencia entre los paquetes de datos con los de voz o de videoconferencia, o cualquier dato que se quiera priorizar. Normalmente el paquete con mayor prioridad es la voz debido aque este se requiere se transmita en tiempo real y el usuario percibiría problemas en la transmisión de manera inmediata; el siguiente es el video y luego los datos.

Este es un pequeño ejemplo de configuración de QoS en un router de prioridad de la voz:

```
class-map match-all VOICE
 match ip precedence 5
!
!
policy-map voice
 class precedence-5
  priority 64
!
interface fastethernet  4
description --- WAN ---
```

ip address x.x.x.x x.x.x.x

service-policy output voice

La configuración de QoS, es muy amplia, por ello esto solo es un ejemplo ilustrativo de su funcionamiento.

Es importante aplicar la política en la interface que se conecta a la WAN de no ser así, el QoS no funcionaria. El **priority** de la política es el ancho de banda asignado a la voz.

Normalmente el proveedor de nuestro servicio, nos informará que tipo de QoS se está aplicando para aplicarla igualmente en nuestro equipo final.

CONCLUSIÓN

Se puede concluir que aplicando los pasos vistos anteriormente se pueden solucionar la mayoría de los problemas que pueda tener una red LAN empresarial. Además se pueden implementar mejoras si se desea aumentar el tamaño de una red LAN y optimizar la utilización de los recursos de la red que posea una empresa.

Se puede estar en la capacidad de formular soluciones a una empresa la cual le genere mayor utilidad al mejorar considerablemente las comunicaciones, es importante impulsar la modernización de las redes empresariales, muchas de estas se encuentran muy desactualizadas y olvidadas. Conforme una empresa crece se requiere el crecimiento de la red empresarial y por consiguiente un mejoramiento de esta.

Podemos estar en la capacidad de determinar problemas en una red LAN empresarial; aplicando las herramientas vistas anteriormente; aplicar la implementación de redundancia en los canales principales y la utilización de Spanning tree, como procesos preventivos ante una caída del canal principal.

Cuando se presente crecimiento de la red LAN empresarial, o cuando se requiera de algún tipo de enrutamiento se estará en la capacidad de poder configurar y verificar el funcionamiento de este.

Con la implementación en la red LAN empresarial de NAT, Firewall, la utilización de programas Sniffer y Network View; podremos tener un monitoreo y control de la red LAN empresarial; gracias a esto se aprovechara al máximo los recursos y no abra malgasto de ancho de banda en actividades o información que corra por la red, diferente a la requerida o utilizada por la empresa y de haber alguna falla esta podrá ser identificada en un corto tiempo para poder solucionarla con el menor impacto posible en las comunicaciones de la empresa.

BIBLIOGRAFIA

- http://www.aprenderedes.com/2006/11/15/bucles-de-capa-2/
- http://aprenderedes.com/2010/03/video-practica-5-configuracion-de-ospf/
- http://www.cisco.com/en/US/products/ps9146/products_ios_technology_home.html
- http://www.guillesql.es/Articulos/Manual_Cisco_CCNA_Protocolos_Enrutamiento.aspx
- http://www.howstuffworks.com/firewall.htm
- http://www.t2app.com/util-ip/nat.htm