Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Diseño, Implementación, Administración y Enrutamiento Avanzado bajo el núcleo IOS CLI (CISCO)

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Jesús Alberto Tejedor Doria

Tutor: Sara Blanco Clavero, Juan Vicente Capella

2013/2014

ÍNDICE

1. CAPÍTULO 1
Preámbulo

1.1 Introducción.

En la actualidad el intercambio de información es algo que esta presente en nuestro día a día, que necesitamos y con lo que no podríamos subsistir, se puede hablar de intercambio de información a todos los niveles, desde la comunicación básica basada en un emisor y un receptor, la comunicación basada entre un emisor y múltiples receptores. Pero que ocurre **¿Cuando el intercambio de información es entre millones de emisores y receptores?.**

Actualmente no podemos hablar de intercambio de información sin pensar en las tecnologías, Internet o todo los que nos rodea constantemente, el conjunto de todo esto tiene un nombre: “redes de telecomunicaciones”.

Cuando definimos el concepto de red de telecomunicación en el mundo de la informática, se define como: *Se entiende por “red de telecomunicación al conjunto de medios (transmisión y conmutación), tecnologías (procesado, multiplexación, modulaciones), protocolos y facilidades en general, necesarios para el intercambio de información entre los usuarios de la red.*

Para poder realizar estos intercambios de información de la manera mas optima debemos seguir una serie de procedimientos, normativas y estándares que sean los adecuados para obtener el mayor rendimiento.

1.2 Definición.

En este proyecto abarcaremos el diseño, implementación y administración de una red de área local con conexiones externas a nivel de campus, no nos centraremos en los servicios, sino en el diseño de la red, recursos que necesitamos para implementarla y su administración.

El proyecto se basa en el diseño de una parte de la red de área local de la Universidad Politécnica de Valencia mediante una simulación con el programa Cisco Packet Tracer. El proyecto esta fraccionado en 5 partes:

- **Memoria:** Contiene toda la información para la implementación de la red, protocolos usados, comandos de implementación, diagramas.
- **Planos:** Contiene los planes del diseño de la red y de su implementación.
- **Pliego de condiciones**
- **Presupuestos:** Tablas con el material necesario y un calculo de costes.
- **Mediciones:** Contiene las simulación del funcionamiento de los distintos protocolos

La simulación de la red contendrá distintas partes del diseño de la red de la universidad, para la implementación y administración de la red se usaran dispositivos de interconexión tales como:

- Routers Catalyst 2811.
- Routers para fibra óptica.
- Routers linkys inalambricos WRT300N.
- Switches catalyst S2000.

Para la implementación de la red se usaran una serie de protocolos justificando su utilización, los protocolos que serán implementados son los siguientes:

- RIPv2.
- OSPF.
- STP.
- VLAN's.
- VTP
- Trunks (protocolo 802.1 Q).
- EthernetChannel.
- FRAME RELAY
- Wireless.
- TFTP
- HTTP.
- NAT.
- PAT.

Los diferentes puntos de la red que se simularan a partir del diseño de la universidad son:

- ETSINF (como diseño de un edificio a partir de los planos).
- El CPD (biblioteca) Como Capa Core de la red
- El backup (centro de investigación)
- Rectorado (Interconexiones de fibra)
- Conexión con distintas escuelas (Arquitectura, Bellas Artes, Caminos, Telecomunicaciones, Informática, Agro nomos). Para la simulación de protocolos.

CAPÍTULO 2
Análisis

La memoria contiene toda la parte de diseño, implementación y administración de la red, explicando como y porque se hace el diseño de la red de una determinada manera, la forma de implementarla y de administrarla.

2.1. Análisis para el diseño de la red.

a) Topología.

A la hora de diseñar una red es conveniente utilizar las topologías de red o estructura física de la red. Las topologías describen la red físicamente y también nos proporcionan la información acerca del método de acceso que se usa (Token Ring, Ethernet, etc). Dado que el diseño esta basado en la red de la universidad vamos a utilizar una topología en estrella.

Una topología en estrella consta de varios nodos conectados a una computadora central (en el caso de la universidad la computadora central es el CPD que se encuentra debajo de la biblioteca central). En un diseño en estrella los mensajes de cada nodo de la red pasan directamente a la computadora central, que determinará, hacia dónde encaminarlos, por lo que finalmente se convierte en una topología mixta, topología en estrella combinada con topología en Anillo. Algunas de las partes de la red se verán como una topología en estrella extendida o árbol.

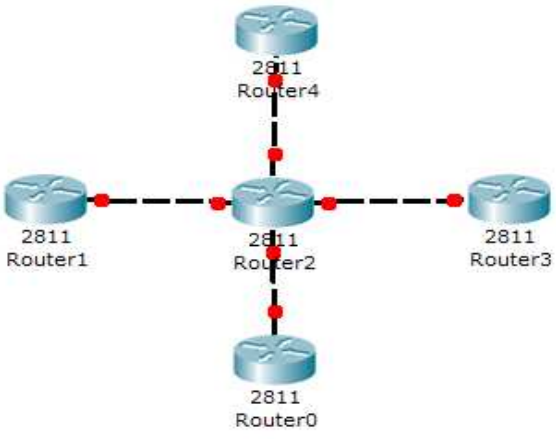


Figura 2.1-1: Topología estrella

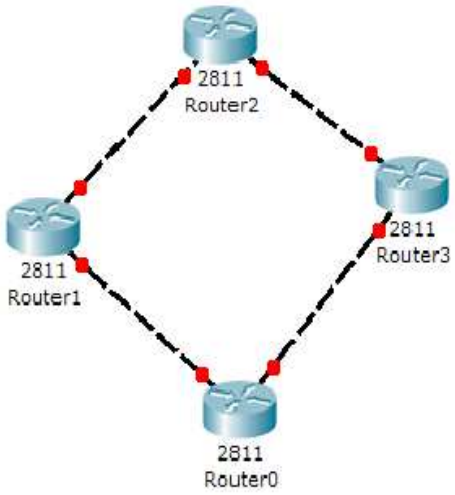


Figura 2.1-2: Topología Bus

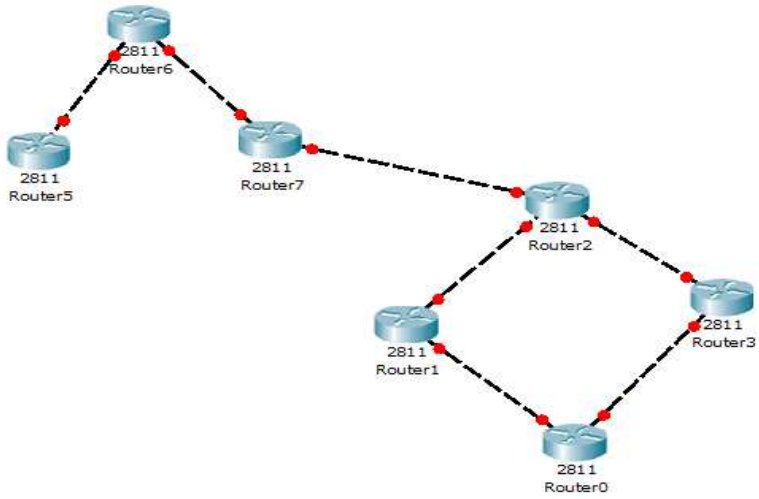


Figura 2.1 -3: topología mixta

Debido al tamaño de la red de la universidad, no se encaminara todo el trafico a la capa core del CPD sino que se delegara parte del encaminamiento a otros routers repartidos por el campus.

- Posible problemas de un mal diseño de la red.
  - Perdida de información:

    La perdida de información se puede producir por muchos factores distintos, desde intrusos en la red hasta un mal diseño o implementación. Algunos de los factores por una implementación son:
    - Caídas de la red: Estas caídas de la red se deben en la mayoría de los casos a una mala conexión con el Servidor, concentradores o una mala conexión con el ISP.
    - Procesamiento lento: Esto puede ser debido a que no se ha elegido el hardware adecuado o no se ha contando con el tamaño de la red.

b) Protocolos.

- TCP/IP:

El protocolo TCP/IP es el protocolo mas extendido en el mundo de las telecomunicaciones y siempre se habla de este protocolo como uno solo pero realmente son dos protocolos que trabajan juntos para transmitir datos: el Protocolo de Control de Transmisión (TCP) y el Protocolo de Internet (IP).

La función del protocolo del protocolo TCP/IP es fragmentar los datos en pequeños paquetes, cuando los paquetes llegan a su destino, se vuelven a su destino de des-fragmentan y vuelven a su forma original.

El protocolo TCP divide los datos en paquetes y los reagrupa cuando llegan a su destino, mientras que le protocolo IP es el encargado de manejar el encaminamiento de los datos y se asegura de que llegan al destinatario correcto.

Norma EIA/TIA 568:

Esta es la norma creada para la instalación de Telecomunicaciones para Edificios Comerciales, que puedan soportar un ambiente productor y proveedores múltiples. En nuestro caso aunque estemos hablando de la red de la universidad tenemos unos usuarios a los que ofrecer servicios por lo tanto estamos hablando de una empresa mas.

El propósito de este estándar es permitir el diseño e instalación del cableado de telecomunicaciones contando con poca información acerca de los sistemas que posteriormente se instalaran. Las instalaciones de los sistemas de cableado durante el proceso de instalación y/o remodelación son significativamente más baratos e implican menos interrupciones que después de que el edificio este finalizado.

La norma EIA/TIA 568A específica los requerimientos mínimos para el cableado de establecimientos comerciales de oficinas. Se hacen recomendaciones para:

- Las topología
- La distancia máxima de los cables

- El rendimiento de los componentes
- Las tomas y los conectores de telecomunicaciones

Se pretende que el cableado de telecomunicaciones especificado soporte varios tipos de edificios y aplicaciones de usuario. Se asume que los edificios Tienen las siguientes características:

- Una distancia entre ellos de hasta 3 Km.
- Un espacio de oficinas de hasta 1,000,000 m2
- Una población de hasta 50,000 usuarios individuales

Las aplicaciones que emplean los sistemas de cableado de telecomunicaciones incluyen, pero no están limitadas a:

- Voz , Datos, Texto, Vídeo, Imágenes

La vida útil de los sistemas de cableado de telecomunicaciones especificados por esta norma debe ser mayor de 10 años.

Los beneficios que nos proporciona la norma son: Flexibilidad, Asegura compatibilidad de Tecnologías, Reduce Fallas, Traslado, adiciones y cambios rápidos.

Centrándonos en el diseño de la UPV

2.2 Implementación de la red

A la hora de implementar una red hay que tener en cuenta una cantidad de requisitos previos para poder proveer a la red de todo lo necesario para un funcionamiento optimo. Los pasos adecuados a seguir para lograr una buena implementación:

1. **Conocimientos previos**
   - Análisis y diseño de sistemas.
   - Legales (Leyes, códigos, reglamentos, convenios, ordenanzas, etc).
   - Técnicos (tecnologías actuales y disponibilidad del mercado).
   - Servicios de Redes (proveedores de servicios de comunicaciones).

2. Descripción de la solicitud de red

- Planteo del Problema (causas por las cuales se solicita la red)

  Información necesaria:

  - Tareas que desarrolla la empresa.
  - Planos de la planta o plantas y vistas de los edificios.
  - Identificación de cada sector.
  - Suministro y distribución de energía eléctrica.
  - Red telefónica.
  - Sistemas de seguridad y protecciones (pararrayos, puesta a tierra, instalaciones de grupos electrógenos, si los hubiera, etc).
  - Riesgos (inundaciones incendios, etc).

3. **Investigación de la empresa solicitante**

- **Relevamiento:**

  a) Elaborar las planillas para el revelamiento.
  b) Detalles de equipos existentes.
  c) Instalaciones preexistentes (no solo de computadoras previamente instaladas).
  d) Datos estadísticos
     - Cantidad de transacciones, locales y remotas.
     - Cantidad de llamadas telefónicas por motivos operativos y administrativos entre los distintos sectores de la empresa.
     - Uso de correo electrónico.
     - Detalles de la secuencia de operaciones (ordenes de compra, fabricación, deposito, expedición, etc).

4. Definición de la red

Proyecto

a) Selección del equipamiento de usuario.
b) Selección del equipamiento de conectividad necesario.
c) Evaluación de la contratación de servicios de terceros.
d) Determinación de alternativas.
e) Relación costo/beneficio.
f) Análisis de impacto y futuro crecimiento.

- Estudio de factibilidad.
- Diseño definitivo. Confección de los planos definitivos
- Proyectos alternativos.
- Presupuestos.
- Aprobación y/o aceptación del solicitante.

5. Instalación de la red

Planificación y programación de tareas.

Coordinación.

Determinación de los tiempo de instalación.

Planes de compra y contrataciones de los medios, equipos y servicios.

Instalación.

- Cableado.
- Equipos de conectividad.
- Equipos de usuario.

Puesta en marcha.

Pruebas de funcionamiento.

Entrenamiento al personal

Aprobación

Entrega de los sistemas funcionando.

Capitulo 3
Memoria

Una vez hemos visto todos los requerimientos previos para la fase de análisis y fase de implementación vamos a proceder a la implementación física de la real con los dispositivos de interconexión necesarios para la implementación de la red de la universidad.

3.1 Planos ETSINF

Figura 3.1 – 1 Plano universidad

Las conexiones troncales de fibra óptica van desde el edificio 3A (Rectorado) hasta el edificio 4L (Biblioteca)

Vamos a comenzar el diseño de la red por la facultad de informática, concretamente por el edificio de la ETSINF.

Es un edificio con cuatro plantas:

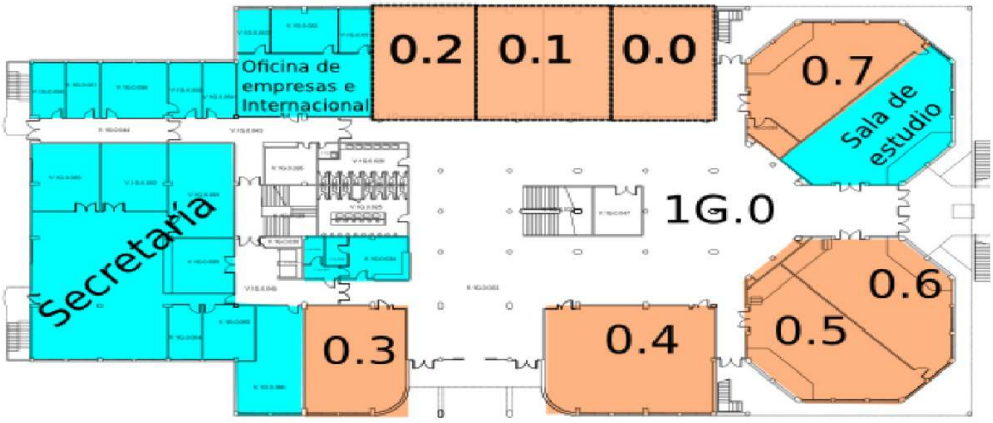


Figura 3.1 - 2 Planta baja Etsinf

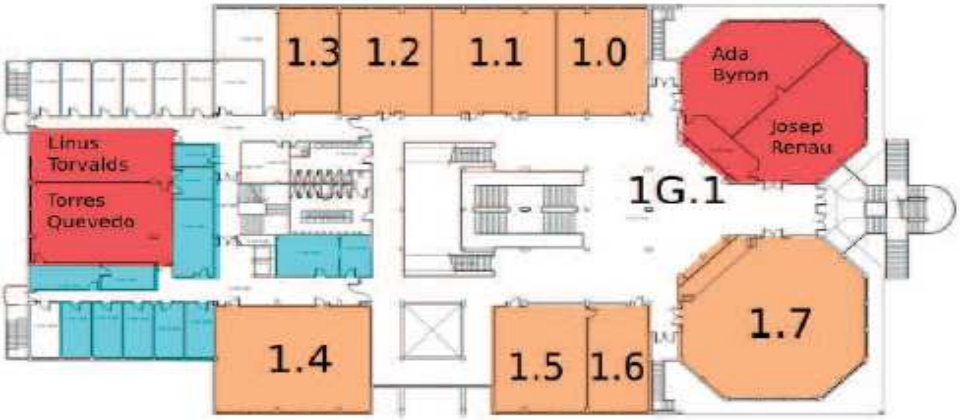


Figura 3.1 - 3 Primera planta Etsinf

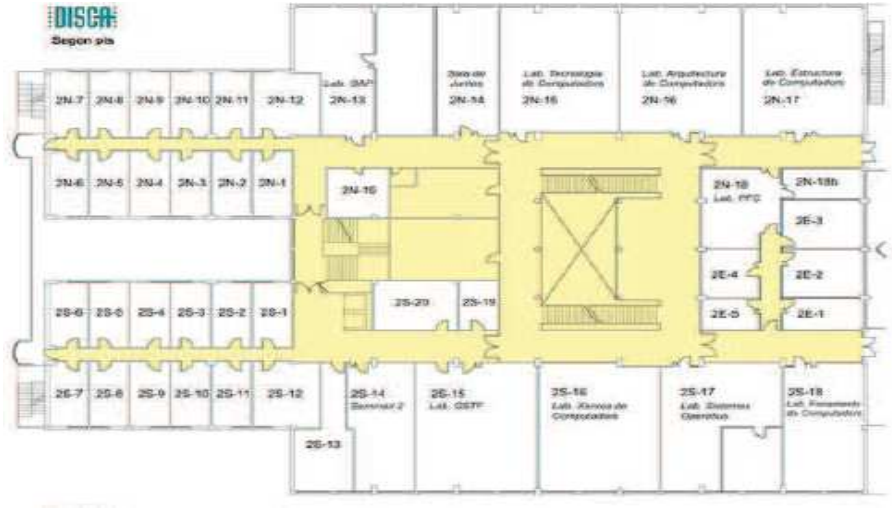


Figura 3.1 -4 Segunda planta Etsinf

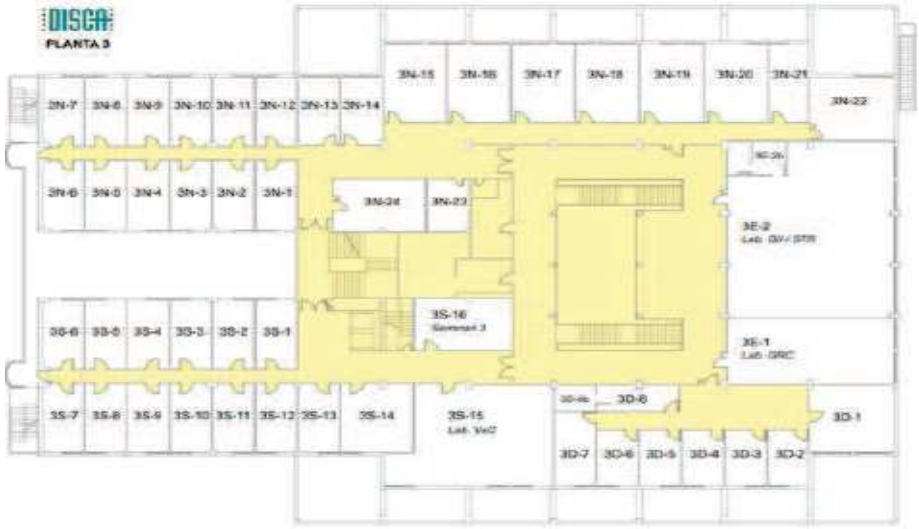


Figura 3.1 - 5 Tercera planta Etsinf

En la facultad de la ETSINF edificio 1G vamos a implementar el diseño de una red de área local, en esta parte del diseño de la red vamos a configurar los switches encargados de la distribución de las vlan's de la facultad.

Vamos a configurar los siguientes protocolos:

- VTP (Vlan trunnking protocol) : Para administración y distribución de VLAN's.
- Etherchannel: para obtener mas ancho de banda y seguridad.
- SPT (Spanning Tree) : Gestión de bucles
- DHCP relay : Proxy para reenviar peticiones de DHCP.

La siguiente figura muestra como quedaría el diseño de la red de la facultad, mostrando solo la parte central, sin contar con todos los switch de las aulas, despachos, laboratorios, etc.

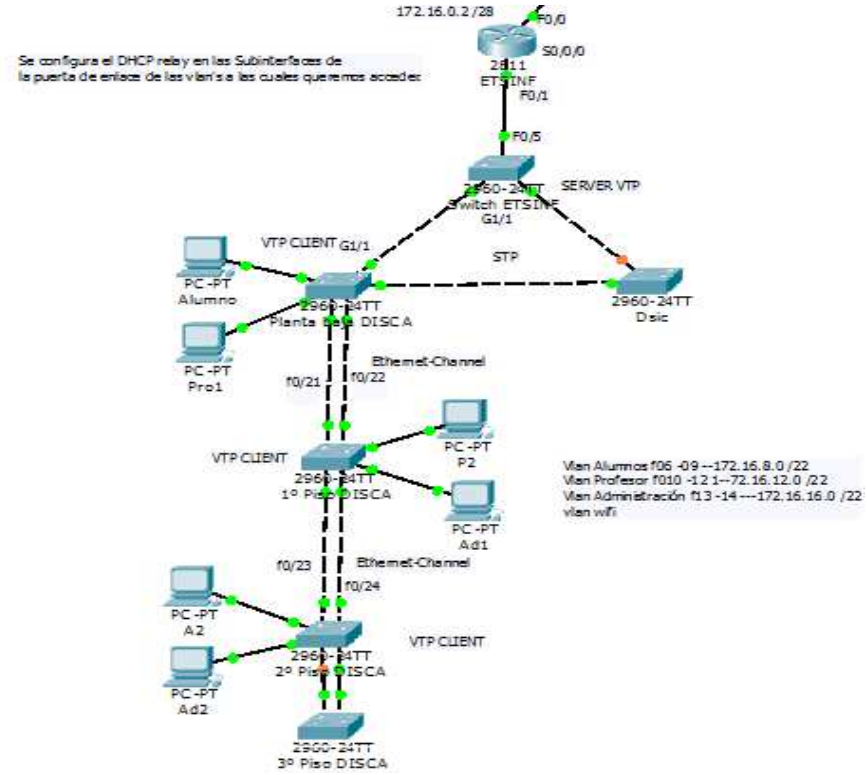


Figura 3.1 – 6 Diseño ETSINF

Antes de comenzar con la configuración de los dispositivos vamos a revisar los comandos básicos para el manejo de los switches de cisco de la serie 2000.

3.2 Comandos básicos switches

Acceso a modos de configuración

- Para ir al modo EXEC Usuario:
  Conectarse al Switch por consola y en el hyperterminal introducir la contraseña inicial esta contraseña se define en contraseña de consola
  S1>

- Para ir al modo EXEC privilegiado:
  Introducir "enable" y la contraseña para este modo (Este es un modo de visualización)
  La contraseña de este modo se define en contraseña secret

  S1> enable
  S1#>

- Para ir al modo Configuración Global:
  Introducir "configure terminal" en el modo EXEC privilegiado (Este es un modo de configuración)

  S1# configure terminal
  S1(config)#

- Para ir al modo de configuración de puertos (desde el modo de configuración global):
  Se accede con el comando "interface" espacio y el puerto o VLAN a configurar, una vez dentro del modo
  interface meteríamos los comandos a realizar para ese Puerto o VLAN.

  S1(config)# interface VLAN1
  S1(config-if)#

  S1(config)# interface fa0/18
  S1(config-if)#
  Para salir del modo de configuración se utiliza el comando "end " o " exit "

1º Configurar el nombre de host del switch

(El comando es "hostname" seguido de un espacio y el nombre que se le quiera dar)

>enable

S1# configure terminal o conf t
S1(config)# hostname CustomerSwitch

2º Configurar la contraseña del modo privilegiado y secret

La contraseña secret es la que da acceso al modo EXEC privilegiado, se activa con el comando "enable secret" seguido de un espacio y la contraseña que le queramos dar.

S1(config)# enable password cisco
S1(config)# enable secret class

3º Configurar la contraseña de consola

La contraseña para ir al modo EXEC se establece en line console 0 y con el comando "password" seguido de un espacio y la contraseña que le queramos poner, se introduce también el comando "login" para que pida la contraseña al acceder..

S1(config)# line console 0
S1(config-line)#
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)#exit

4º Configurar la contraseña de vty

La contraseña para acceso remoto (acceso por Telnet una vez configurada la IP del Switch) se configura en line vty 0 15, con el comando "password" seguido de un espacio y la contraseña deseada, se introduce también el comando "login" para que pida la contraseña al acceder, para encriptar estas contraseñas se hace con el comando "service password-encryption" en el modo de Configuración global.

S1(config)# line vty 0 15
S1 (config-line)#

```
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)# service password-encryption
```

5º Configurar una dirección IP en la interfaz VLAN99 o la que especifiquemos

Se accede con el comando "interface" seguido de un espacio y el nombre de la VLAN a la que queremos poner una IP (sera la VLAN por la que accederemos remotamente al switch), seguidamente le asignamos una IP con el comando "ip address" seguido de un espacio, la IP, otro espacio y la mascara deseada, activamos esta interfaz con el comando "no shutdown".

```
S1(config)#interface VLAN 99
S1(config-if)#ip address 192.168.1.5 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
```

6º Configurar el gateway por defecto

Para el envió de tramas a internetwork (salir de la Red LAN local al exterior mediante un Router) se debe asignar la IP de la interfaz LAN del router por medio del gateway del switch con el comando " ip default-gateway" seguido de un espacio y la IP del Router al que se conecta.

```
S1(config)# ip default-gateway 192.168.1.1
```

7º Para guardar el contenido del archivo de configuración en ejecución en la RAM no volátil

(NVRAM), se ejecuta el comando "copy running-config startup-config".

```
S1# copy running-config startup-config
```

Nota: Siempre que se hagan configuraciones en el switch, se deberá guardar una copia de seguridad en la NVRAM y ejecutar el comando copy running-config startup-config, para garantizar que los cambios realizados no se pierdan, si el sistema se reinicia o apaga. Guardar el archivo de seguridad con otro nombre util si se quiere tener varias versiones (se pone también un ejemplo llamando al archivo prueba)

S1# copy startup-config flash:"nombre de archivo"
S1#copy startup-config flash:prueba.bak1

Restauración de un archivo de configuración guardado: Se copia un archivo guardado como archivo de inicio y se ejecuta reload para que se reinicie el switch y cargue el nuevo archivo de configuración.

S1# copy flash: prueba.bak1startup-config flash: prueba.bak1
S1# reload

Copia de respaldo de los archivos de configuración en un servidor TFTP

Se utiliza una IP y nombre de archivo a modo de muestra

S1# copy system:running-config tftp://172.16.2.155/tokyo-config

Restauración de archivo de configuración de un servidor TFTP.

Se utiliza una IP y nombre de archivo a modo de muestra

S1# copy tftp://172.16.2.155/tokyo-config system:running-config

3.3 VTP (Vlan Trunking Protocol)

Es un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un domino de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos. El protocolo VTP nace como una herramienta de administración para redes de cierto tamaño, donde la gestión manual se vuelve inabordable.

VTP opera en 3 modos distintos:

- Servidor
- Cliente
- Transparente

Servidor:

Es el modo por defecto. Desde él se pueden crear, eliminar o modificar VLANs. Su cometido es anunciar su configuración al resto de switches del mismo dominio VTP y

sincronizar dicha configuración con la de otros servidores, basándose en los mensajes VTP recibidos a través de sus enlaces **trunk**. Debe haber al menos un servidor. Se recomienda autenticación MD5.

Cliente:

En este modo no se pueden crear, eliminar o modificar VLANs, tan sólo sincronizar esta información basándose en los mensajes VTP recibidos de servidores en el propio dominio. Un cliente VTP sólo guarda la información de la VLAN para el dominio completo mientras el switch está activado. Un reinicio del switch borra la información de la VLAN.

Transparente:

Desde este modo tampoco se pueden crear, eliminar o modificar VLANs que afecten a los demás switches. La información VLAN en los switches que trabajen en este modo sólo se puede modificar localmente. Su nombre se debe a que no procesa las actualizaciones VTP recibidas, tan sólo las reenvía a los switches del mismo dominio.

Los administradores cambian la configuración de las VLANs en el switch en modo servidor. Después de realizar cambios, estos son distribuidos a todos los demás dispositivos en el dominio VTP a través de los enlaces permitidos en el *trunk* (VLAN 1, por defecto), lo que minimiza los problemas causados por las configuraciones incorrectas y las inconsistencias. Los dispositivos que operan en modo transparente no aplican las configuraciones VLAN que reciben, ni envían las suyas a otros dispositivos. Sin embargo, aquellos que usan la versión 2 del protocolo VTP, enviarán la información que reciban (publicaciones VTP) a otros dispositivos a los que estén conectados con una frecuencia de 5 minutos. Los dispositivos que operen en modo cliente, automáticamente aplicarán la configuración que reciban del dominio VTP. En este modo no se podrán crear VLANs, sino que sólo se podrá aplicar la información que reciba de las publicaciones VTP.

Para que dos equipos que utilizan VTP puedan compartir información sobre VLAN, es necesario que pertenezcan al mismo dominio. Los switches descartan mensajes de otro dominio VTP.

Las configuraciones VTP en una red son controladas por un número de revisión. Si el número de revisión de una actualización recibida por un switch en modo cliente o servidor es más alto que la revisión anterior, entonces se aplicará la nueva configuración. De lo contrario se ignoran los cambios recibidos. Cuando se añaden nuevos dispositivos a

un dominio VTP, se deben resetear los números de revisión de todo el dominio VTP para evitar conflictos. Se recomienda tener mucho cuidado al usar VTP cuando haya cambios de topología, ya sean lógicos o físicos. Realmente no es necesario resetear todos los números de revisión del dominio. Sólo hay que asegurarse de que los switches nuevos que se agreguen al dominio VTP tengan números de revisión más bajos que los que están configurados en la red. Si no fuese así, bastaría con eliminar el nombre del dominio del switch que se agrega. Esa operación vuelve a poner a cero su contador de revisión.

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

Configuración del switch para la red de la UPV.

Como podemos observar en la figura 3.1 - 5 Diseño ETSINF, en la facultad tenemos diferentes plantas en las cuales tenemos tanto en la planta baja como en la primera, despachos en la primera, segunda y tercera, etc. Por lo tanto tenemos que distribuir las diferentes vlan's a lo largo de todo el edificio y para eso usamos el protocolo VTP ya que nos permite distribuir y administrar las vlan's sin necesidad de configurarlas en todos los dispositivos de la red.

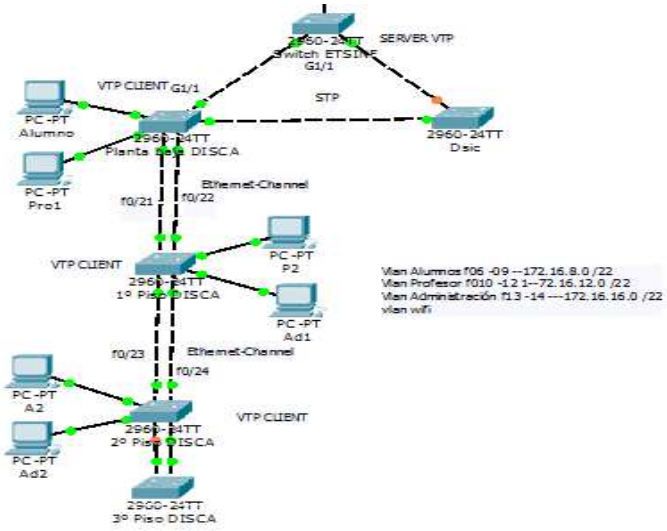


Figura 3.3 – 1, Configuración VTP

1º Lo primero que tenemos que hacer es configurar el switch que va a ser el servidor VTP, que en nuestro caso es el switch frontera de la facultad, “swicth ETSINF”. Entramos en la consola del switch y en modo configuración y lanzamos los siguientes comandos:

Etsinf(config)#vtp mode [MODO] → Seleccionamos el modo **“server”**
Etsinf(config)#vtp domain [DOMINIO] → Dominio **“Etsinf”**

Etsinf(config)#vtp password [CONTRASEÑA] → password “**etsinf”**

Acto seguido creamos las diferentes vlan's para la facultad la escuela de informática, vamos a crear una vlan para alumnos, profesores y administración

Switch#vlan database
Switch(vlan)#vlan [número de vlan] **“2”** name [nombre de vlan] **“alumnos”**
Switch(vlan)#exit
realizamos el mismo paso para la vlan de **profesores** (vlan **“3”**) y la vlan de **administración** (vlan **“4”**).

En este caso no necesitamos asignar una vlan a un puerto, dado que podríamos decir que es el switch de la capa core y simplemente se encarga de administrar y desplegar las vlan's.

Para que las vlan's puedan ser desplegadas a lo largo de la red debemos poner las interfaces que están conectadas entre los switches en modo trunk.

Switch(config)#interface fastethernet G1/1
Switch(config-if)#switchport mode trunk

La configuración debe quedar de la siguiente manera:

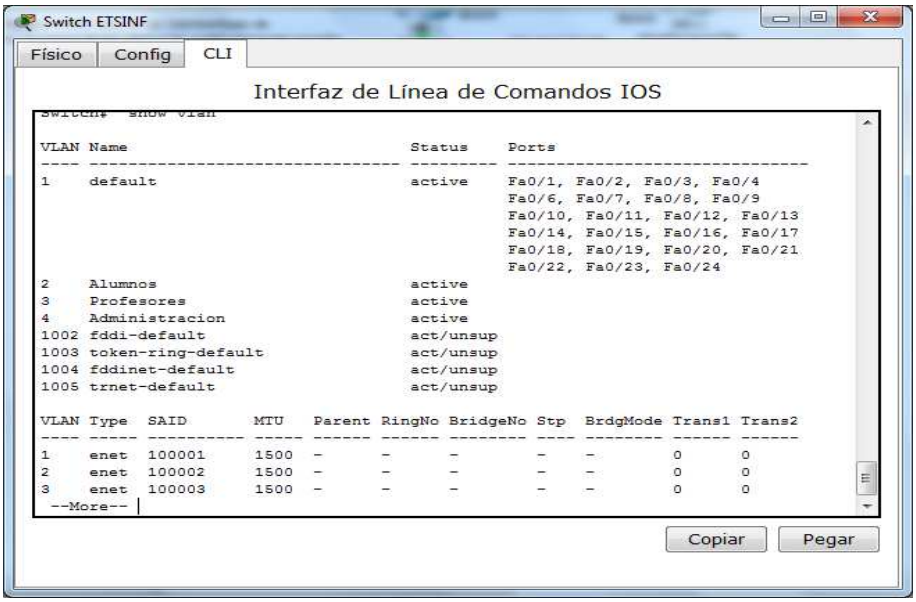


Figura 3.3 – 2 Configuración vtp

Podemos ver en la figura 3.1 -7 las vlan's creadas correctamente pero no hemos asignado ninguna interfaz.

2º Ahora vamos a uno de los switch del edificio de la etsinf para configurarlo en modo cliente, vamos al switch **"planta baja disca"** entramos en la configuración y lo ponemos en modo cliente para que se desplieguen las vlan's del servidor.

Etsinf(config)#vtp mode [MODO] → Seleccionamos el modo "Client"
Etsinf(config)#vtp domain [DOMINIO] → Dominio "Etsinf"
Etsinf(config)#vtp password [CONTRASEÑA] → password "etsinf"

Y acto seguido configuramos configuramos las interfaces que están conectadas entre los switches en modo trunk. Ahora si tenemos que asignar las vlan's a las diferentes interfaces con el siguiente comando:

Switch(config)#interface [Interfaz] "**f0/6"**
Switch(config-if)#switchport access vlan [número de vlan] **"2"**

Ahora en la interfaces fastethernet 0/6 esta asignada la vlan 2 de alumnos, debemos aplicar la misma configuración para la interfaces 0/10 para la vlan 3 de profesores y así para todas las interfaces que estén siendo desplegadas por el server vtp.

Si queremos asignar una vlan a un grupo de interfaces lanzaremos el siguiente comando.

Switch(config)#interface range [Interfaz] "f0/6 – f0/10"

3º Una vez tenemos configurado el servidor VTP y los respectivos clientes, tenemos que añadir un router para el enrutamiento entres las distintas vlan's y que cada vlan tenga su puerta de enlace.

Pero antes de empezar a configurar el router vamos a listar los comandos básicos de los routers cisco de la serie 2800.

3.2 Comandos básicos router

1º cambiar el nombre del host:

Router(config)# hostname

2º Borrar la configuración del router:

#erase nvram: (debe confirmarse con enter una segunda vez)

3º Salvar la configuración del router:

#copy running-config startup-config

4º Reiniciar el enrutador: (Es normal que pida salvar los cambios de configuración no guardados)

#reload

#Proceed with reload? [confirm]

5º Asignar ip a una interfaz

(config)#interface
(config-if)#ip address

6º Visualizar la configuración del router:

#show running-config

7º Visualizar la tabla de enrutamiento de un router:

#show ip route

8º Visualizar el estado de todas las interfaces:

#show interfaces

9º Visualizar el estado de una interfaz:

#show interface <#>

10º Establecer el password del modo enable:

(config)#enable password

11º Establecer el password encriptado: (Es normal que arroje una alerta si se establece la misma clave para el enable password)

(config)#enable secret

12º Habilitar la encripción de claves en el archivo de configuración:

(config)#service password-encryption

13º Habilitar las terminales virtuales:

(config)#line vty <#1> <#1>

(config-line)#password

(config-line)#login

3.5 Configuración del router ETSINF

El router ETSINF es el router por el cual saldrá el trafico de la escuela hacia el exterior o hacia otros dispositivos de la red.

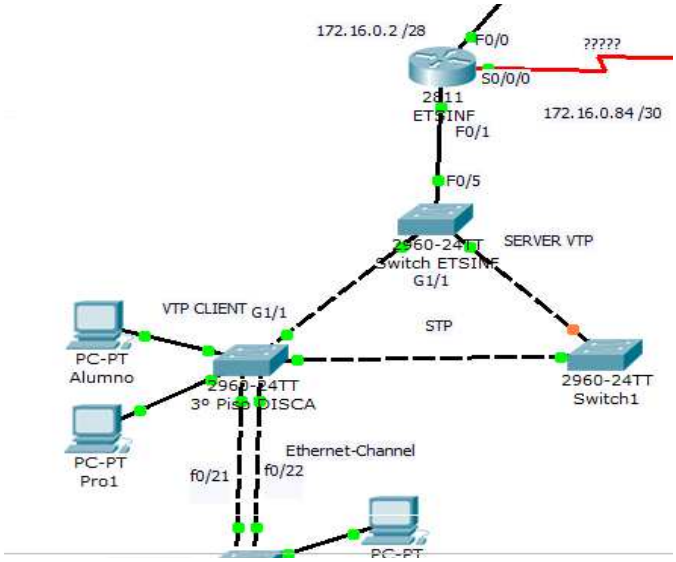


Figura 3.5 – 1 Config router ETSINF

Vamos a configurar este router para que las distintas vlan's tengan conexión entre ellas, para ellos debemos de ir a la interfaz donde esta conectado el switch server y configurar las distintas sub-interfaces para que las distintas vlan's tengan su puerta de enlace y el router pueda aplicar el enrutamiento.

Accedemos al router en modo configuración y lanzamos los siguientes comandos:

router(conf-t)# interfaces fastEthernet f0/1.1 → accedemos a la subinterface

router(conf-sub-if)# ip a a 172.16.8.1 255.255.255.0 → asignamos ip + mac a la sub- interface

router(conf-sub-if)#encapsulation dot1Q "num" → activamos la encapsulación y el numero de encapsulación.

router(conf-sub-if)#no shutdown → levantamos la sub-interface

Realizamos la misma configuración para cada una de las sub-interfaces de las distintas vlan's.

3.6 DHCP Relay

El "Agente de Retransmisión de DHCP" o "DHCP Relay Agent" es una servidor o router configurado para escuchar broadcasts DHCP de clientes DHCP y reenviar esos mensajes a los servidores DHCP en diferentes subredes. Los agentes de retransmisión son parte de los estándares DHCP y funciona según los documentos estándar Request for Comments (RFCs) que describen el diseño del protocolo y el comportamiento relacionado. Así que por curiosidad un "RFC 1542-Compliant Router" es un router que soporta el reenvío de tráfico DHCP broadcast.

Como hemos comentado los clientes DHCP utilizan broadcasts para obtener la concesión de una IP en un servidor DHCP. Los Routers normalmente no pasan broadcasts excepto que estén configurados específicamente para dejarlos pasar. Por lo tanto, sin configuración adicional los servidores DHCP solo proveen direcciones IP a clientes en su red local. Para que podamos asignar direcciones a clientes en otros segmentos, debemos configurar la red para que los DHCP broadcasts puedan llegar desde el cliente al servidor DHCP.

Esto se puede hacer de dos maneras: configurando los routers que conectan las subnets para dejar pasar DHCP broadcasts, o configurando el "Agente de Retransmisión" o DHCP Relay Agents.

2. Configuración

Como podemos ver en la siguiente figura tenemos el servidor DHCP fuera de nuestra del rango de la etsinf por lo tanto vamos a necesitar un agente dhcp relay para poder realizar las peticiones de dhcp a un servidor dhcp externo.

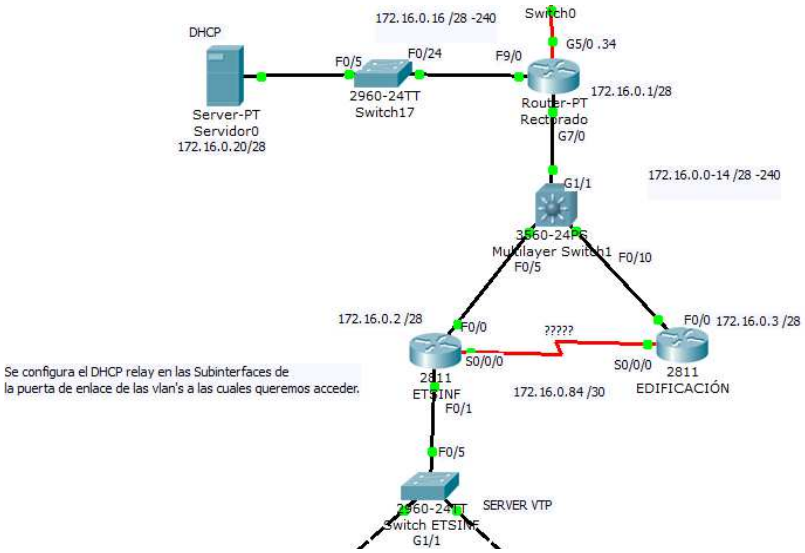


Figura 3.6 – 1 Config DHCP relay

Como hemos mencionado con anterioridad el servidor DHCP esta fuera de la red de las vlan's de la facultad de informativa, por lo que vamos a configurar el dhcp relay. Previamente deberemos de haber creado los pools de dhcp en el servidor.

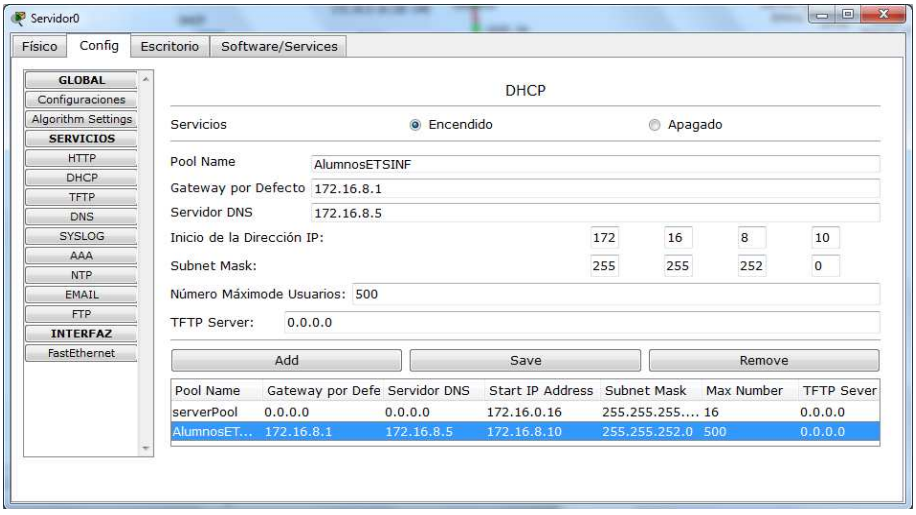


Figura 3.6 – 2 Config DHCP Server

Para configurar el dhcp relay accedemos a la consola del router etsinf y accedemos a cada una de las sub-interfaces creadas anteriormente y lanzamos los siguiente comandos:

router(conf-t)# interfaces fastEthernet f0/1.1 → accedemos a la subinterface
router(conf-sub-if)# ip helder-address 127.16.0.20 → la dirección ip del servidor dhcp al cual queremos realizar la petición.

Nota: Debemos realizar esta acción para cada una de las sub-interfaces. La configuración debe quedar como la siguiente:

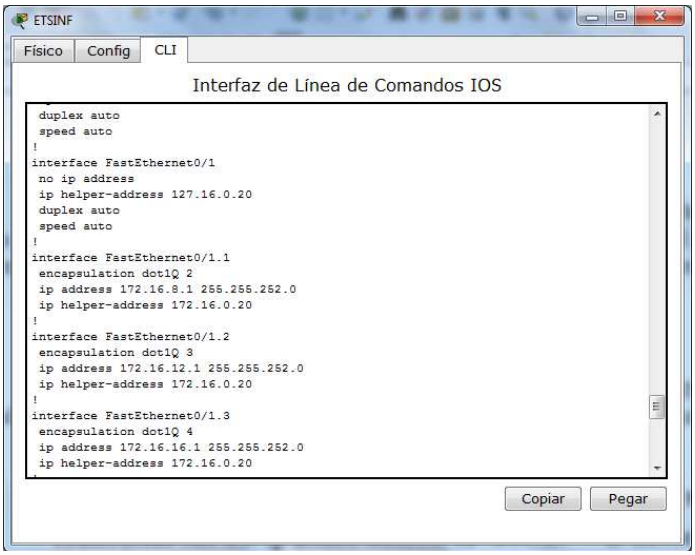


Figura 3.6 – 3 Config router etsinf

3.7 Ethernet Channel

EtherChannel es una tecnología de Cisco construida de acuerdo con los estándares 802.3 full-duplex Fast Ethernet. Permite la agrupación lógica de varios enlaces físicos Ethernet, esta agrupación es tratada como un único enlace y permite sumar la velocidad nominal de cada puerto físico Ethernet usado y así obtener un enlace troncal de alta velocidad.

Un máximo de 8 puertos Fast Ethernet, Giga Ethernet o 10Gigabit Ethernet pueden ser agrupados juntos para formar un EtherChannel. Con esta última agrupación es posible conseguir un máximo de 80 Gbps de ancho de banda. Las conexiones EtherChannel pueden interconectar switches, routers, servidores o clientes.

Los puertos usados deben tener las mismas características y configuración.

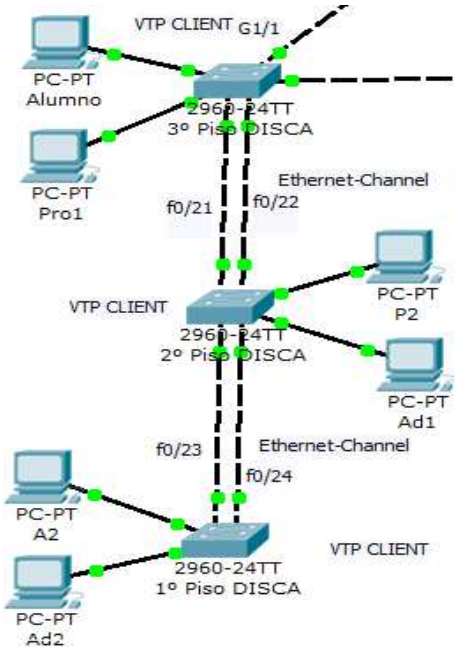


Figura 3.7 – 1 Config Ethernet Channel

Al implementar esta tecnología en nuestra red no solo estamos doblando el ancho de banda sino que ademas estamos si la fusionamos con el protocolo STP (Spanning tree) obtenemos enlaces con el doble de ancho de banda y ademas con la opción de tenerlos en stamby para futuras caídas.

Para configurar el ethernet channel accedemos a la linea de comandos del switch “3º piso disca” en modo configuración y lanzamos las siguientes ordenes:

Switch(conf-t)# int range fastEthernet 0/21- 0/22 → Seleccionamos el rango de interfaces que están conectadas al switch del segundo piso.

Switch(conf-int-range)#channel-group 1 mode active → Creamos un nuevo puerto que engrosa esas 2 interfaces y se crea un port channel.

Switch(conf-t)# int port channel “num” → Nos metemos en la configuración del puerto channel y el numero de puerto asignado.

Switch(int-port)# switchport mode trunk → activamos el modo trunk para que se puedan seguir desplegando las vlan's.

Hay que realizar la misma operación para todas las interfaces de todos los switch que están conectados en la troncal del edificio, aumentando así el ancho de banda en las conexiones verticales entre las distintas plantas.

3. 8 Spanning Tree

En comunicaciones, STP (del inglés Spanning Tree Protocol) es un protocolo de red de nivel 2 del modelo OSI (capa de enlace de datos). Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice la eliminación de bucles. STP es transparente a las estaciones de usuario.

El algoritmo transforma una red física con forma de malla, en la que existen bucles, por una red lógica en forma de árbol (libre de bucles). Los puentes se comunican mediante mensajes de configuración llamados Bridge Protocol Data Units (BPDU).

El protocolo establece identificadores por puente y elige el que tiene la prioridad más alta (el número más bajo de prioridad numérica), como el puente raíz (Root Bridge). Este puente raíz establecerá el camino de menor coste para todas las redes; cada puerto tiene un parámetro configurable: el Span path cost. Después, entre todos los puentes que conectan un segmento de red, se elige un puente designado, el de menor coste (en el caso que haya el mismo coste en dos puentes, se elige el que tenga el menor identificador "dirección MAC"), para transmitir las tramas hacia la raíz. En este puente designado, el puerto que conecta con el segmento, es el puerto designado y el que ofrece un camino de menor coste hacia la raíz, el puerto raíz. Todos los demás puertos y caminos son bloqueados, esto es en un estado ya estacionario de funcionamiento.

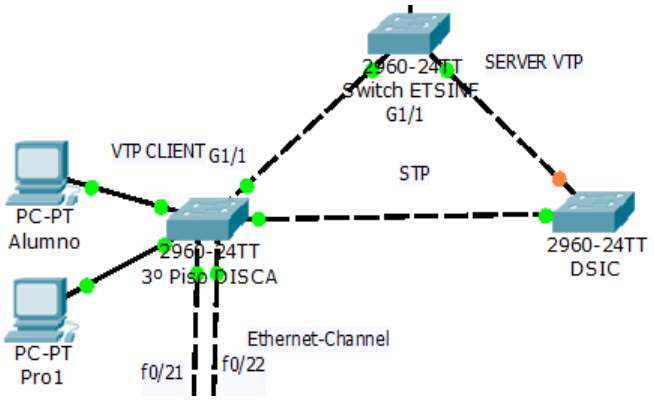


Figura 3.8 – 1 Config Spanning Tree

Como podemos ver en la figura 3.1 – 10 hay 3 switches conectados entre si formando un bucle, por lo que para ir a un mismo sitio tenemos dos caminos distintos, el problema surge cuando se cierra la malla y entonces tenemos un bucle, gracias a la implementación del STP tenemos el enlace desde el switch “etsinf” hasta el switch “dsic” en stamby, este enlace esta esperando una caída de alguno de los otros enlaces que forman el camino para levantarse y dar servicio.

Para implementar el protocolo Spanning Tree accedemos al switch del “dsic”, entramos en el modo de configuración de la consola y lanzamos los siguiente comandos:

Switch(conf-t)# spanning-tree vlan “num” root primary/secundary → activa el modo root primario o secundario.
Switch(conf t)# spanning-tree vlan “num” priority “num_priordidad” → ponemos el numero de prioridad de la vlan seleccionada, siendo 1 la mayor prioridad.

Si lo seleccionamos como secundario veremos como el cable se queda en stamby y si lo ponemos en modo primario veremos como cambiamos los roles y otro de los enlaces se pone en stamby.

Nota: tenemos que realizar la misma operación para todo la malla y así configurarlo de forma que conozca todas las reglas a seguir, también cabe decir, que los switches cisco activan el spanning tree por defecto.
Por otra parte deberíamos de realizar la misma operación si configuramos el STP en un puerto etherchannel y deberíamos de configurar el SPT bajo el mismo numero de puerto que el etherchannel dado que luego se convierte en un solo cable.

CAPITULO 4

ENRUTAMIENTO

4.1 Protocolos de enrutamiento

Un protocolo de enrutamiento es el esquema de comunicación entre routers. Un protocolo de enrutamiento permite que un router comparta información con otros routers, acerca de las redes que conoce así como de su proximidad a otros routers.

Sistemas autónomos: Un sistema autónomo (AS) es un conjunto de redes bajo una administración común, las cuales comparten una estrategia de enrutamiento común. Los números de identificación de cada AS son asignados por el Registro estadounidense de números de la Internet (ARIN), los proveedores de servicios o el administrador de la red.

La mayoría de algoritmos de enrutamiento pertenecen a una de estas dos características:

- Vector distancia.
- Estado de enlace.

Vector distancia: Protocolos de enrutamiento vector-distancia. Los protocolos de enrutamiento por vector-distancia envían copias periódicas de las tablas de enrutamiento de un router a otro. Los algoritmos de enrutamiento basados en el vector-distancia también se conocen como algoritmos Bellman-Ford. Los protocolos de enrutamiento por vector-distancia:

Estado de enlace: Los protocolos de enrutamiento de estado del enlace mantienen una base de datos compleja, con la información de la topología de la red. Los algoritmos de estado del enlace también se conocen como algoritmos Dijkstras o SPF ("primero la ruta máscorta") El algoritmo de vector-distancia provee información indeterminada sobre las redes lejanas y no tiene información acerca de los routers distantes.

Puntos de interés acerca del estado del enlace.

- **Carga sobre el procesador.**
- **Requisitos de memoria.**
- **Utilización del ancho de banda.**

Vector-distancia vs estado de enlace

Vector-distancia	Estado de enlace
Visualiza la topología de red desde la perspectiva de los vecinos	Obtiene una visión común de la topología de toda la red.
Suma los vector-distancia de router a router	Calcular la ruta más corta a otros routers
Realiza actualizaciones periódicas con frecuencia y su convergencia es lenta	Ofrece actualizaciones desencadenadas por eventos con una convergencia mas rápida
Envía copias de las tablas de enrutamiento a los routers vecinos	Envía actualizaciones de enrutamiento de estado de enlace a otros routers
Usa una topología plana	Permite el diseño jerárquico para grandes internetworks

4.2 RIPV2 (vector-distancia)

RIP son las siglas de Routing Information Protocol (Protocolo de Información de Enrutamiento). Es un protocolo de puerta de enlace interna o IGP (Interior Gateway Protocol) utilizado por los routers (encaminadores) para intercambiar información acerca de redes IP a las que se encuentran conectados. Su algoritmo de encaminamiento está basado en el vector de distancia, ya que calcula la métrica o ruta más corta posible hasta el destino a partir del número de "saltos" o equipos intermedios que los paquetes IP deben atravesar. El límite máximo de saltos en RIP es de 15, de forma que al llegar a 16 se considera una ruta como inalcanzable o no deseable. A diferencia de otros protocolos RIP es un protocolo libre es decir que puede ser usado por diferentes router y no únicamente por un solo propietario, como es el caso de IGRP que es de Cisco Systems.

- Utiliza el puerto 520 UDP
- Protocolo Classless (soporta CIDR)
- Soporta VLSMs
- La métrica es el numero de saltos (el número de Routers que un paquete debe atravesar antes de llegar a su destino.)
- Actualizaciones periódicas de enrutamiento son enviadas cada 30 segundos a la dirección multicast 224.0.0.9
- 25 rutas por mensaje RIP (24 si se utiliza autenticación).
- Soporta autenticación.

- Implementa Split Horizon con Poison reverese.
- Implementa actualizaciones por eventos.
- La mascara de subred es incluida.
- Distancia administrativa es de 120.
- Utilizada en redes pequeñas (flat networks) o al borde de redes grandes

Vamos a configurar el protocolo RIPV2 en nuestra red, vamos a hacer una pequeña simulación de su funcionamiento.

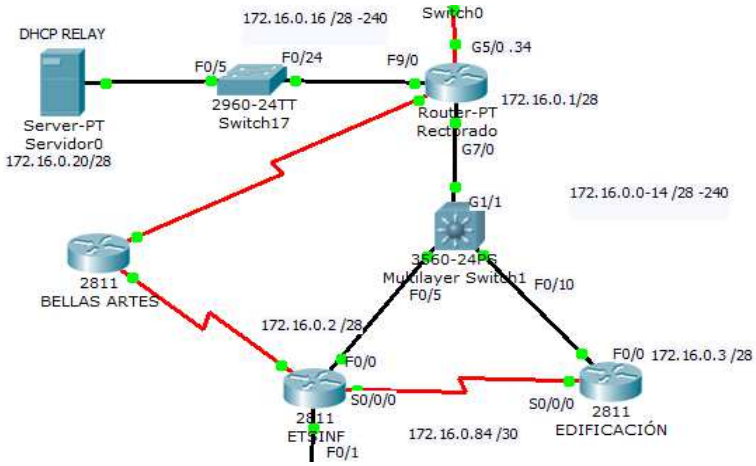


Figura 4.2 – 1 Protocolo RIPV2

Vamos a configurar el protocolo RIPV2 para un conjunto de routers que están en la parte inferior de la red, como ejemplo para demostrar el funcionamiento del protocolo y su configuración.

Accedemos a la linea de comandos del router “Etsinf” y en modo configuración lanzamos las siguientes ordenes:

etsinf(conf-t)# router rip → Habilitamos el protocolo rip
etsinf(conf-t)# version 2 → Activamos la versión 2 del protocolo.
Etsinf (router-rip)# network [red directamente conectadas] → La dirección ip de las redes a las cuales el router esta directamente conectadas.

NOTA: En este caso hay que estar atentos y publicar también las redes de las vlan's que están directamente conectadas en las vlan's.

Lanzando el comando # show ip route → podemos ver la tabla de enrutamiento y debería quedar tal que así:

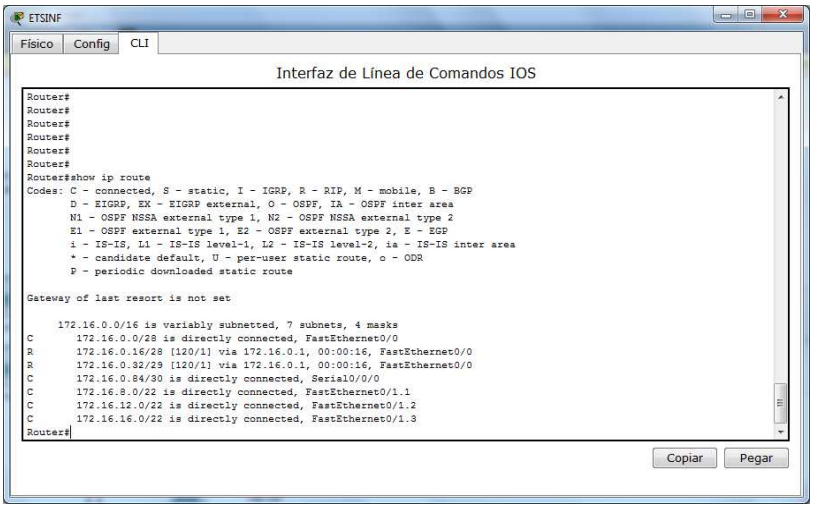


Figura 4.2 – 2 Tabla de enrutamiento

Las rutas representadas con “C”, son las rutas directamente conectadas y las rutas representadas con “R”, son las rutas conocidas a partir del protocolo RIPV2.

4.3 OSPF (estado de enlace)

OSPF Es un protocolo de enrutamiento llamado de estado de enlace que utiliza unos paquetes específicos para conocer dicho estado. Dichos paquetes informativos se llaman LSAs (link-state advertisements), y son enviados a todos los routers dentro del área donde está funcionando. La información en los interfaces conectados, las métricas usadas y otras variables propias de un protocolo de enrutamiento, está incluidas en los LSAs. Los routers OSPF acumulan esta información de estado de enlaces, y usan el algoritmo SPF para calcular la ruta más corta a cada nodo. Como protocolo que mantiene un control del estado de los enlaces en la red, OSPF contrasta con otros protocolos (como el protocolo RIP mencionado antes), es que los existentes son de vector de distancia.

Los routers que funcionan con algoritmos de vector distancia envían toda o parte de sus tablas de rutas en mensajes de actualización a sus vecinos.

A diferencia de otros sistemas de routing, OSPF puede operar dentro de una jerarquía. La entidad más grande dentro de una jerarquía es lo que llamamos sistema autónomo, lo cual se explicó en el apartado anterior sobre los protocolos de enrutamiento. Como explicación rápida, un sistema autónomo (AS) es un grupo de redes bajo una administración común que comparte una estrategia de enrutamiento.

El protocolo OSPF es interno en el AS, aunque es capaz de recibir y enviar rutas a otros sistemas autónomos. Un sistema autónomo puede ser dividido en un número de áreas, los cuales son grupos de redes contiguas con equipos conectados (ordenadores, servidores, etc.). Routers con varios interfaces pueden participar en múltiples áreas. Estos routers, los cuales son llamados ABR (routers fronteras en el área), mantienen bases de datos topológicas separadas para cada área.

Para la red de la universidad hemos simulado un mallado OSPF para ver el funcionamiento del protocolo. El protocolo es el encargado de interconectar los routers frontera de distintas facultades.

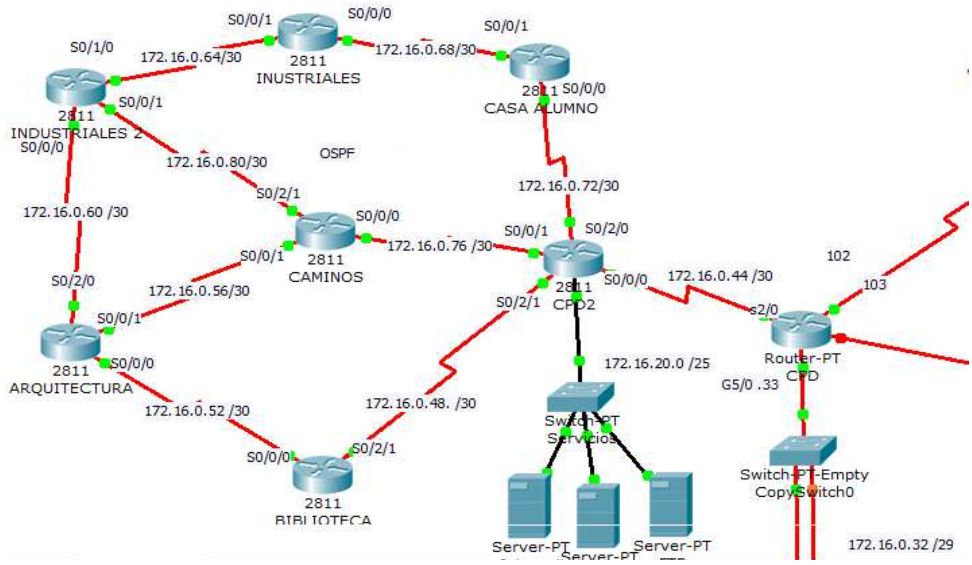


Figura 4.3 – 1 Diseño OSPF

Vamos a configurar el protocolo ospf en el router “CPD2”, accedemos a la linea de comandos en modo configuración y lanzamos los siguientes comandos:

Router(config)#router ospf 1
Router(config-router)#network [direccion de red] wildcard [direccion wildcard] área [num]
Router(config-router)#network 172.16.0.72 0.0.0.3 area 0
Router(config-router)#network 172.16.0.76 0.0.0.3 area 0
Router(config-router)#network 172.16.0.48 0.0.0.3 area 0
Router(config-router)#network 172.16.0.44 0.0.0.3 area 0

Lo que hacemos es en el router "cpd2" activamos el enrutamiento ospf "num" su numero de proceso y luego publicamos las redes a las cuales esta directamente conectado. Esta configuración hay que realizarla en todos los routers de la malla.

La configuración es básicamente similar a la del protocolo ripv2. A diferencia de que el protocolo ospf reacciona cuando hay un cambio en la red, restableciendo otra vez sus rutas en busca de todos los caminos.

Autenticación protocolo OSPF

Vamos a implementar la autenticación del protocolo OSPF entre cada enlace de la red, vamos a realizar un ejemplo entre el router "cpd2" y su enlace con la "casa del alumno".

Figura 4.3 – 2 Autenticación OSPF

Para aplicar esta configuración debemos entrar en el modo consola del router "CPD2" y en la interfaz serial 0/2/0 que es el enlace directamente conectado a la casa del alumno y lanzar el siguiente comando:

Router(config)#int s0/2/0

Router(config-if)#ip ospf message-digest-key 1 md5 7 asecret

Router(config-router)#area 0 authentication message-digest

- Key [1] → Es el numero de proceso.
- Md5 [1 – 7] --> Es el nivel de encriptación
- [asecret] → Es la contraseña

Luego activamos la autenticación con el comando area 0 authentication message-digest [area 0] → es el area donde vamos a introducir la encriptación.

NOTA: Debemos realizar esta configuración para cada uno de los nodos de interconexión.

Conexión entre diferentes áreas

También podemos configurar el protocolo ospf en diferentes área de trabajo y que mediante un router de backbone área. En nuestra red podríamos representar esa configuración poniendo la malla en el área 0 y la conexión frame relay mediante ospf en el área 1.

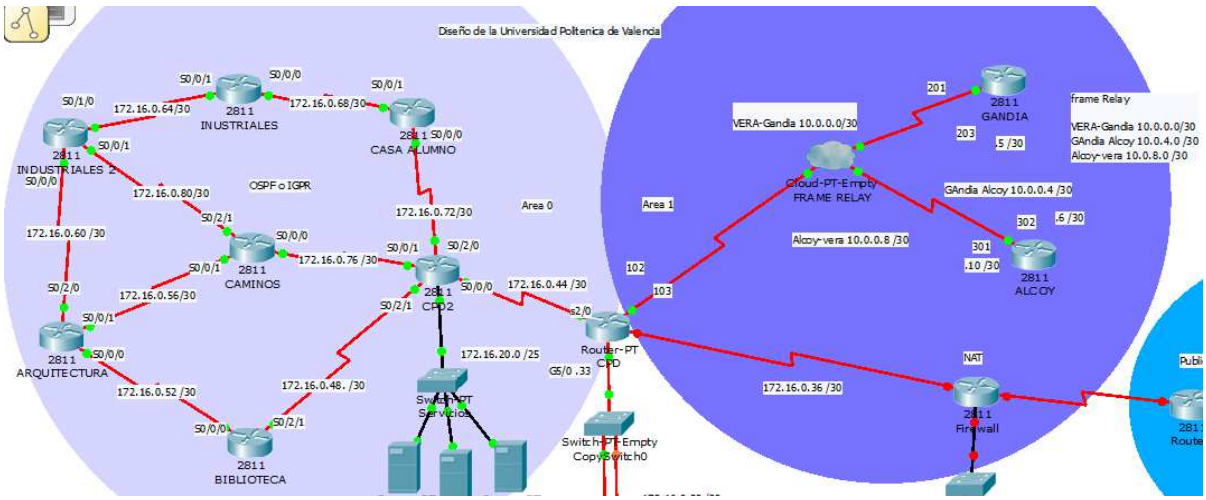


Figura 4.3 – 3 OSPF Areas

Aplicamos esta configuración en el router backbone que en este caso es el CPD para poder conectar las dos áreas lo único que tenemos que hacer es crear un nuevo proceso ospf que contenga las dos áreas como regla.

Router(config)#router ospf 2
Router(config-router)#network 172.16.0.44 0.0.0.3 area 0
Router(config-router)#network 10.0.0.0 0.0.0.3 area 1
Router(config-router)#network 10.0.0.8 0.0.0.3 area 1

Vamos a lanzar el comando show ip route en algunos de los routers de la malla para ver como quedan las tablas de enrutamiento.

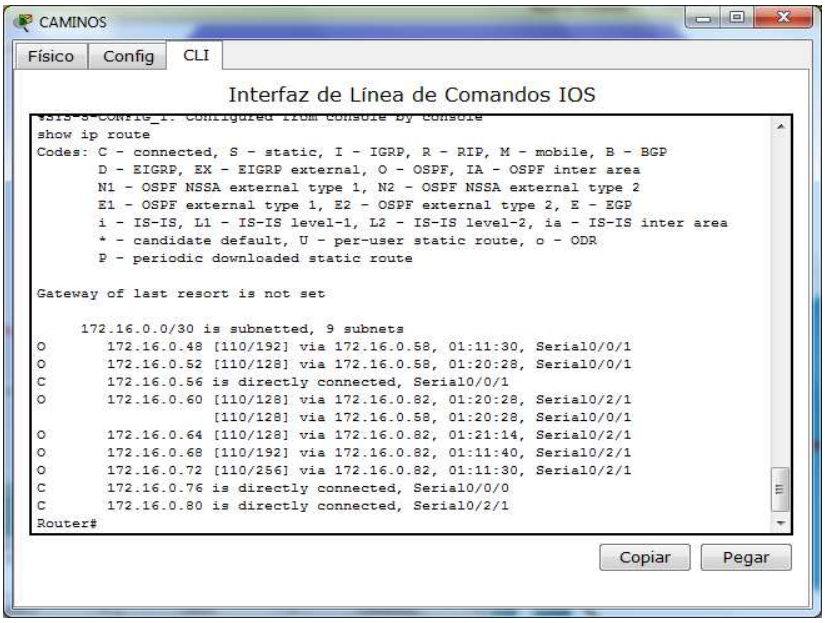


Figura 4.3 – 4 Tabla enrutamiento “Caminos”

Como podemos ver conoce las rutas directamente conectadas “C” y el resto de rutas mediante el protocolo ospf “O” donde nos día mediante que red encuentra el siguiente salto y porque interfaz.

Si listamos el router “CPD2” podemos ver que al listar la tabla de enrutamiento no aparece las rutas conocidas por ospf ya que hemos encriptado las datos que ospf envía a sus vecinos.

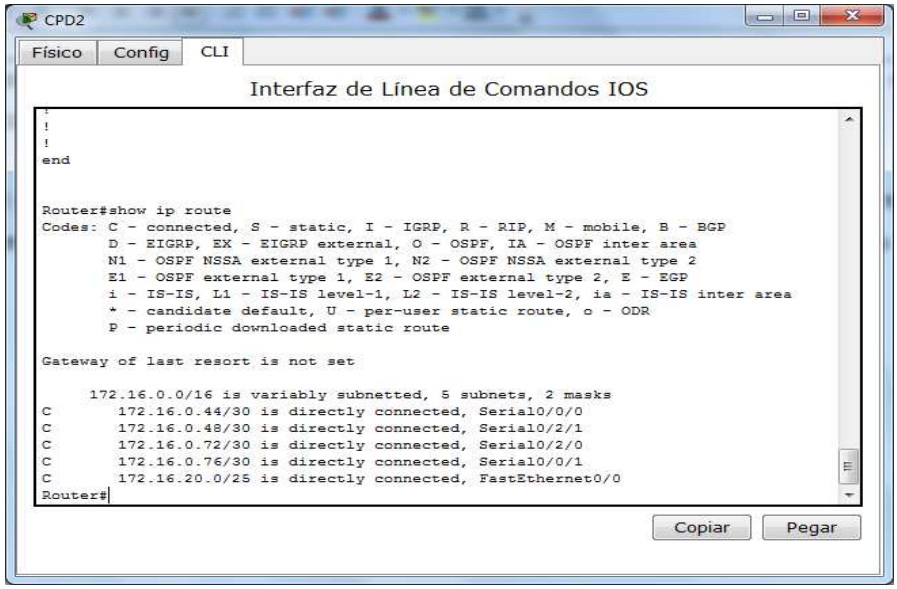


Figura 4.3 – 5 Tabla enrutamiento “CPD2”

CAPITULO 5

CONEXIONES EXTERNAS

En esta parte de la implementación vamos a configurar las conexiones mediante frame relay con el campus de Alcoy y el campus de Gandia.

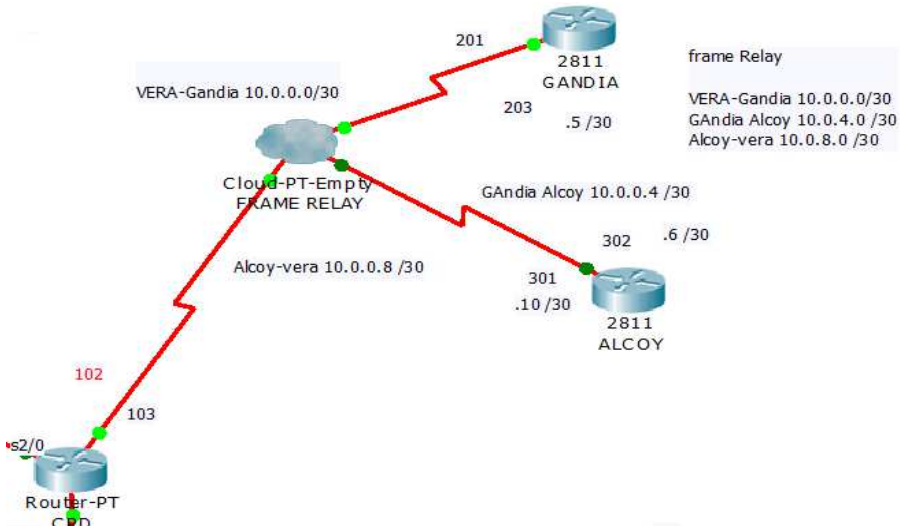


Figura 5.1 – 1 Conexión Frame relay

5.1 Frame relay

La técnica **Frame Relay** se utiliza para un servicio de transmisión de voz y datos a alta velocidad que permite la interconexión de redes de área local separadas geográficamente a un coste menor.

Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada punto a punto, esto quiere decir que es orientado a la conexión.

Las conexiones pueden ser del tipo permanente, (PVC, Permanent Virtual Circuit) o conmutadas (SVC, Switched Virtual Circuit). Por ahora sólo se utiliza la **permanente.** De hecho, su gran ventaja es la de reemplazar las líneas privadas por un sólo enlace a la red. El uso de conexiones implica que los nodos de la red son conmutadores, y las tramas deben llegar ordenadas al destinatario, ya que todas siguen el mismo camino a través de la red, puede manejar tanto tráfico de datos como de voz.

Aplicaciones y Beneficios

- Reducción de complejidad en la red. elecciones virtuales múltiples son capaces de compartir la misma línea de acceso.
- Equipo a costo reducido. Se reduce las necesidades del “hardware” y el procesamiento simplificado ofrece un mayor rendimiento por su dinero.

- Mejora del desempeño y del tiempo de respuesta. penetración directa entre localidades con pocos atrasos en la red.

- Mayor disponibilidad en la red. Las conexiones a la red pueden redirigirse automáticamente a diversos cursos cuando ocurre un error.
- Se pueden utilizar procedimientos de Calidad de Servicio (QoS) basados en el funcionamiento Frame Relay.
- Tarifa fija. Los precios no son sensitivos a la distancia, lo que significa que los clientes no son penalizados por conexiones a largas distancias.
- Mayor flexibilidad. Las conexiones son definidas por los programas. Los cambios hechos a la red son más rápidos y a menor costo si se comparan con otros servicios.
- Ofrece mayores velocidades y rendimiento, a la vez que provee la eficiencia de ancho de banda que viene como resultado de los múltiples circuitos virtuales que comparten un puerto de una sola línea.
- Los servicios de Frame Relay son confiables y de alto rendimiento. Son un método económico de enviar datos, convirtiéndolo en una alternativa a las líneas dedicadas.
- El Frame Relay es ideal para usuarios que necesitan una conexión de mediana o alta velocidad para mantener un tráfico de datos entre localidades múltiples y distantes .
- Opcionales WEB, Libros virtuales: redes.

5.2 Implementación Frame Relay

Para crear la conexión frame relay entre los distintos puntos primero debemos configurar la nube, para que simule una linea dedicada punto a punto.

Figura 5.2 – 1 Enlaces Frame relay

Una vez tenemos configurada la nube con los distintos enlaces serial, nos tenemos que ir a el router “CPD” y configurar las subinterfaces que irán conectadas a cada uno de los destinos. Dado que tenemos dos destinos para la serial 0/0 del router “CPD” debemos crear dos subinterfaces.

Se han etiquetado las rutas con la siguiente enumeración:

Id	Campus	enlaces	ID	Enlace inverso	ID
1	Vera	Vera-Gandia	102	Gandia-Vera	201
2	Gandia	Gandia-Alcoy	203	Alcoy-Gandia	302
3	Alcoy	Alcoy-Vera	301	Vera-Alcoy	103

Tabla 5.2 – 1 Tabla enlaces frame relay

Accedemos al router en modo configuración y lanzamos los siguientes comandos

Router(config)#int s0/0

Router(config-if)#encapsulation frame relay → Activamos la encapsulación para la interface.

Router(config-if)#int s0/0/0.102 point-to-point → Creamos la subinterface con el ID de Vera-Gandia y activamos el point-to-point

Router(config-subif)#ip add 10.0.0.1 255.255.255.252 → Asignamos una dirección.

Router(config-subif)#frame-relay interface-dlci 102 → creamos la conexión frame relay con el identificador dlci

CAPITULO 6

NAT

Existen distintos tipos de versiones de NAT atendiendo a la necesidad de nuestra red.

6. 1 NAT estático

Consiste básicamente en un tipo de NAT en el cuál se mapea una dirección IP privada con una dirección IP pública de forma estática. De esta manera, cada equipo en la red privada debe tener su correspondiente IP pública asignada para poder acceder a Internet. La principal desventaja de este esquema es que por cada equipo que se desee tenga acceso a Internet se debe contratar una IP pública. Además, es posible que haya direcciones IP públicas sin usar (porque los equipos que las tienen asignadas están apagados, por ejemplo), mientras que hay equipos que no puedan tener acceso a Internet (porque no tienen ninguna IP pública mapeada).

6. 2 NAT dinámico

Este tipo de NAT pretende mejorar varios aspectos del NAT estático dado que utiliza un pool de IPs públicas para un pool de IPs privadas que serán mapeadas de forma dinámica y a demanda. La ventaja de este esquema es que si se tienen por ejemplo 5 IPs públicas y 10 máquinas en la red privada, las primeras 5 máquinas en conectarse tendrán acceso a Internet. Si suponemos que no más de 5 máquinas estarán encendidas de forma simultánea nos garantiza que todas las máquinas de nuestra red privada tendrán salida a Internet eventualmente. Para configurar este tipo de NAT definimos el pool de IPs públicas disponibles y el rango de direcciones privadas que deseamos que sean mapeadas.

6. 3 NAT con sobrecarga

El caso de NAT con sobrecarga o PAT (Port Address Translation) es el más común de todos y el más usado en los hogares. Consiste en utilizar una única dirección IP pública para mapear múltiples direcciones IPs privadas. Las ventajas que brinda tienen dos enfoques: por un lado, el cliente necesita contratar una sola dirección IP pública para que las máquinas de su red tengan acceso a Internet, lo que supone un importante ahorro económico; por otro lado se ahorra un número importante de IPs públicas, lo que demora el agotamiento de las mismas.

La pregunta casi obvia es cómo puede ser que con una única dirección IP pública se mapeen múltiples IPs privadas. Bien, como su nombre lo indica, PAT hace uso de múltiples puertos para manejar las conexiones de cada host interno.

6.4 Implementación NAT con sobrecarga

Dado el volumen de nuestra red vamos a utilizar un configuración pasada en **Nat con sobrecarga o Pat**, aunque hay que mencionar que en grandes redes se usan pool's de direcciones publicas.

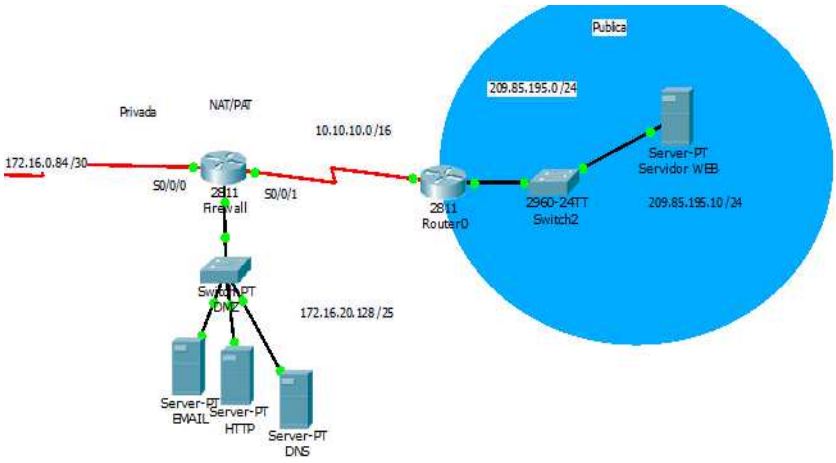


Figura 6.4 -1 Nat

Para configurar el Nat con sobrecarga accedemos a la linea de comandos del router "firewall" y lanzamos los siguientes comandos:

Router(config)#int s0/0/1
Router(config-if)#ip add 10.10.10.1 255.255.0.0
Router(config-if)#no shutdown
Router(config-if)#int s0/0/0
Router(config-if)#ip add 172.16.0.86 255.255.255.253
Router(config-if)#ip access-list standard internet
Router(config-std-nacl)#permit 172.16.0.84 0.0.0.3
Router(config-std-nacl)#exit
Router(config)#ip nat inside source list internet interface serial 0/0/1 overload

```
Router(config)#int s0/0/0
Router(config-if)#ip nat inside
Router(config-if)#int s0/0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
```

1. **ip nat inside**: es el comando que se utiliza para ingresar los comando asociados con NAT

2. Source list internet: Estamos definiendo las direcciones IP que queremos natear. Al ingresar source list estamos haciendo referencia a una lista de acceso. Por último internet se refiere al nombre que le colocamos a la lista de acceso en el paso anterior.

3. interface serial 0/0/1: Se refiere a la interfaz que tiene la dirección IP pública.

4. overload: Este comando mágico es el que crea el PAT. Esto es lo que permite que el bloque completo de direcciones IPs definidas en la lista de acceso pueda salir con una única dirección IP pública.

Por último tenemos que definir cual es la interfaz de la LAN y cual es la de la WAN. Esto lo hacemos con los comandos ip nat inside e ip nat outside.

CAPITULO 7

WIRELESS

En una red del tamaño de la red de la universidad y en los tiempos que corren no podía faltar la tecnología wireless. Para instalar el wireless en la universidad debemos tener en cuenta diferentes factores:

1. Dispositivos
   - Estaciones móviles
   - AP (Access Point)
   - Bridge: Une dos redes a nivel de capa 2. Se configura un AP como bridge entre una red 802.11 y una red Ethernet.

2. Estandar 802.11
   - Direct Sequence Spread Spectrum (DSSS) en la banda ISM de 2.4 Ghz.
   - DSS esparce la señal en una banda de 22MHz logrando alguna inmunidad respecto a la interferencia.
   - Potencia máxima 100mW
   - Ancho de banda que se ajusta a 1Mbps, 2 Mbps, 5.5 Mbps o 11Mbps dependiendo de la calidad del enlace
   - El BW efectivo en una Wlan no es mas de 4 o 5 Mbps.
   - El alcance maximo varia entre 20m y 300m dependiendo de implementaciones especificas.
   - El protocolo de acceso al medio es CSMA/CA.

3. Protocolos
   - Los adaptadores no utilizan FEC (Forward Error Correction)
   - Los adaptadores Lucent WaveLAN 802.11b, utilizan protocolos ARQ con 4 retransmisiones como máximo.
   - Las tarjetas que cumplen con el estándar se demoninan Wi-Fi.

4. Requerimientos de Diseño
   - Una red de área local inalámbrica (WLAN) tiene los siguientes requerimientos básicos:
     - Cobertura completa en el área determinada
     - Capacidad suficiente para soportar el trafico.
   - Los requerimientos anteriores cumple a través de :

- Ubicación adecuada de los AP
- Asignación adecuada de canales.

5. Barrera de Transmisión

- Madera, plástico y vidrio no es problema.
- Concreto y ladrillos pueden ser barreras significativas
- En un ambiente abierto se puede alcanzar 300m sin problema, pero a 20 o 60 metros cuando hay oficinas.

6. Mediciones

- No existen reglas simples de calculo. Es necesario medir.
- Hay que hacer pruebas exhaustivas y poner especial énfasis en aspectos de propagación para lograr cubrir el área de interés.
- Especial cuidado en el interior de un recinto ya que es un espacio tridimensional.
- Un AP podría cubrir dos pisos dependiendo de los materiales de construcción.

7. Algunas reglas de diseño

- Espaciar lo máximo posible los AP asegurando cobertura completa del área.
- Red de un piso: usar canales: 1, 6 y 11 para evitar toda interferencia inter-canal.
- Red de varios pisos: Usar canales: 1, 4, 7 y 11 para limitar las interferencia inter-canal.
- Red de un piso: canales: 1, 6 y 11 para evitar que dos AP adyacentes usen el mismo canal.
- Red de varios pisos: canales: 1, 4 7 y 11 para evitar que canales adyacentes usen el mismo canal.

5. Procedimiento de diseño

- Ubicar inicialmente los AP

- Ajustar las ubicaciones de los AP basados en mediciones de intensidad de señal.
- Construir un mapa de cobertura.
- Asignar canales de frecuencia a los AP basado en el mapa de cobertura.

7.1 Roaming

Es la capacidad de una estación móvil de desplazarse físicamente sin perder comunicación. Se logra configurando varios AP en una red ESS de forma tal de no perder servicio. Se configura conectando varios AP a la misma subred física.

Para montar un punto de acceso se configuran los puntos de acceso como bridges. Para optimizar el desempeño, configurar la densidad del punto de acceso como High, Medium, Low dependiendo cuan lejos están unos de otros. Fijar la densidad a High permite mayor ancho de banda porque se fuerza a la estación móvil busca un nuevo si se baja de 11 Mbps.

- **High: máxima distancia entre AP – 30m**
- **Medium: máxima distancia entre AP – 60m**
- **Low: máxima distancia entre AP – 120m**

El funcionamiento del roaming se basa en que el servidor DHCP en la subred Ethernet proporciona IP a los equipos móviles, la estación móvil retiene la Ip al cambiar de un BSS a otro. Las tablas en los puntos de acceso en modo “Bridge” que definen los equipos móviles activos son actualizadas cuando una estación móvil se mueve entre AP (“hand off”)

Para la red de la universidad implementamos puntos de acceso en modo bridge formando un roaming.

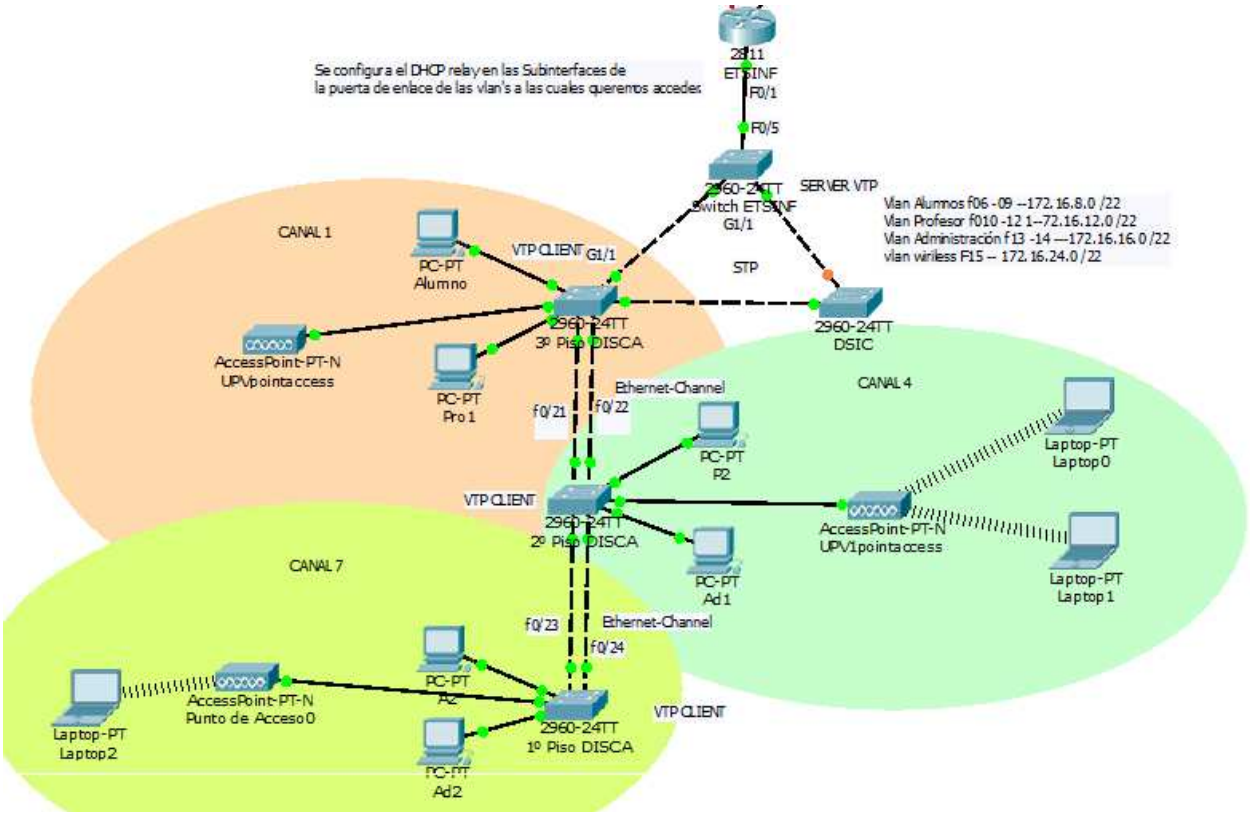


Figura 7.1 – 1 – Roaming wireless

7. 2 Implementación wireless

1º Accedemos al switch “ETSINF” y creamos una nueva vlan “100” name “wireless” , como este switch tiene el protocolo VTP habilitado en modo server automáticamente tenemos la vlan desplegada por todos los switch que estén dentro del mismo dominio.

2º Accedemos al router frontera de la ETSINF y creamos una subinterface como puerta de enlace para la Vlan 100 wireless con IP 172.16.24.1 255.255.255.240.

3º Accedemos al servidor DHCP encargado del pool del wireless que en este caso esta en el CPD, con dirección IP: 172.16.20.10 /25. Como esta fuera de nuestra red debemos activar el ip helper-address en la subinterface de la vlan 100 y decirle cual es nuestro servidor dhcp.
4º Asignamos las interfaces de los switches a la vlan 100.

```
Swicth(conf t)# int fastEthernet 0/15
```

Swicth(conf-int)# switchport mode access

Swicth(conf-int)# switchport access vlan “100”

5º Instalamos los puntos de acceso en esas interfaces que están asignadas a la vlan 100 “wireless”.

6º Configuramos los puntos de acceso.:

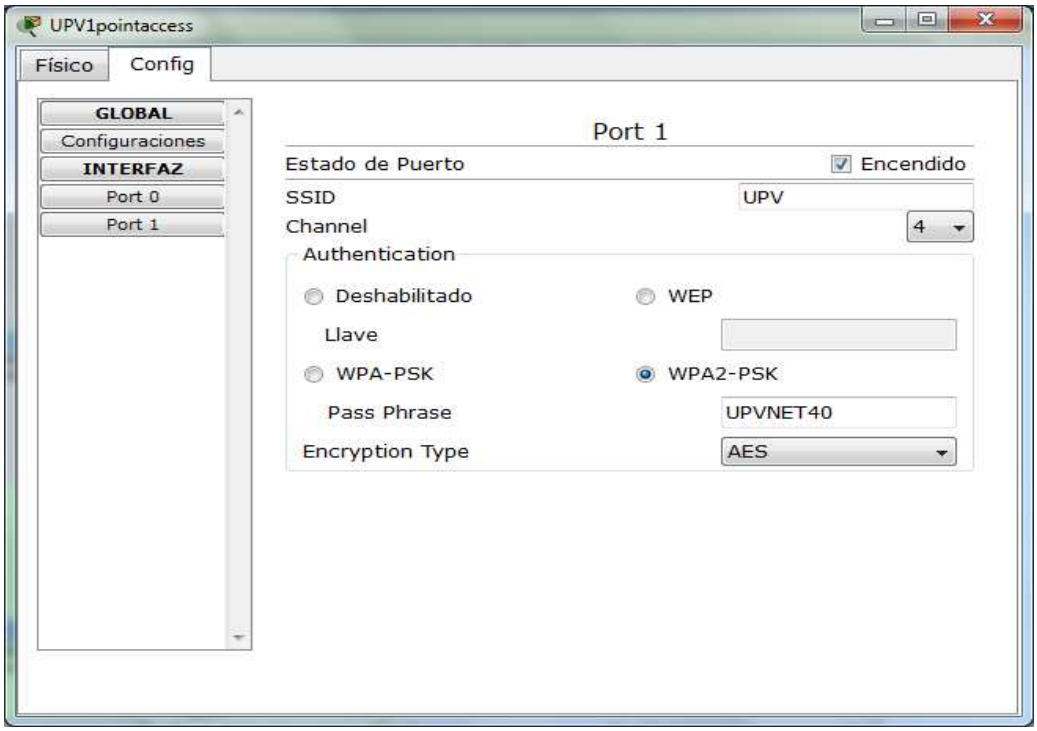


Figura 7.2 -1 Configuración AP

SSID: Mismo SSID para los puntos de acceso: UPV

Seguridad de tipo WPA2_PSK con encriptacion **AES** : UPVNET40

7º Conectar los terminales móviles a el punto de acceso.

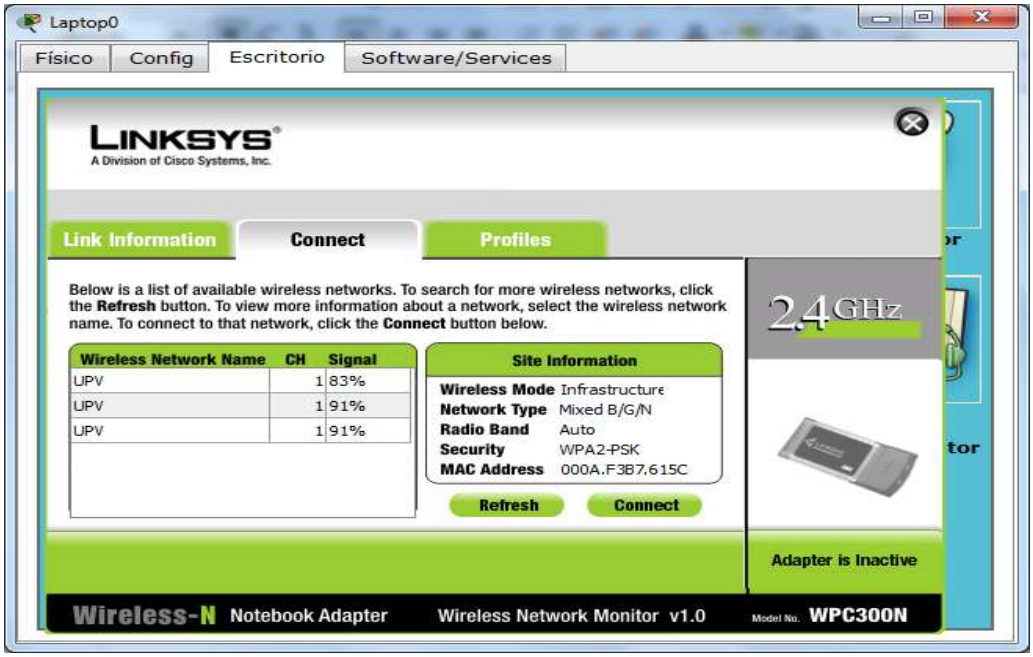


Figura 7.2 – 2 Redes inalambricas

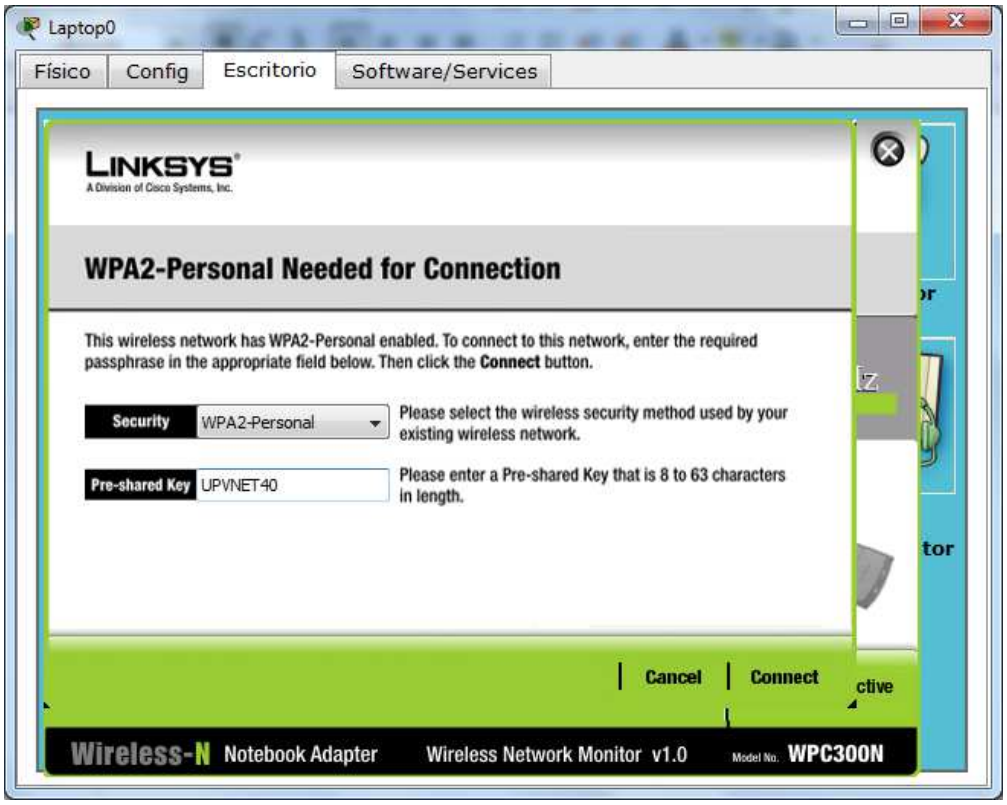


Figura 7.2 – 3, Credenciales

CAPITULO 8

TFTP

COMO SERVIDOR DE BACKUP

8.1 TFTP

son las siglas de Trivial file transfer Protocol (Protocolo de transferencia de archivos trivial).

Es un protocolo de transferencia muy simple semejante a una versión básica de FTP. TFTP a menudo se utiliza para transferir pequeños archivos entre ordenadores en una red, como cuando un terminal X Window o cualquier otro cliente ligero arranca desde un servidor de red.

Algunos detalles del TFTP:

- Utiliza UDP (en el puerto 69) como protocolo de transporte (a diferencia de FTP que utiliza los puertos 20 y 21 TCP).
- No puede listar el contenido de los directorios.
- No existen mecanismos de autenticación o cifrado.
- Se utiliza para leer o escribir archivos de un servidor remoto.
- Soporta tres modos diferentes de transferencia, "netascii", "octet" y "mail", de los que los dos primeros corresponden a los modos "ascii" e "imagen" (binario) del protocolo FTP.

Detalles de una sesión TFTP

Ya que TFTP utiliza UDP, no hay una definición formal de sesión, cliente y servidor, aunque se considera servidor a aquel que abre el puerto 69 en modo UDP, y cliente a quien se conecta.
Sin embargo, cada archivo transferido vía TFTP constituye un intercambio independiente de paquetes, y existe una relación cliente-servidor informal entre la máquina que inicia la comunicación y la que responde.

- La máquina A, que inicia la comunicación, envía un paquete RRQ (read request/petición de lectura) o WRQ (write request/petición de escritura) a la máquina B, conteniendo el nombre del archivo y el modo de transferencia.
- B responde con un paquete ACK (acknowledgement/confirmación), que también sirve para informar a A del puerto de la máquina B al que tendrá que enviar los paquetes restantes.
- La máquina origen envía paquetes de datos numerados a la máquina destino,

todos excepto el último conteniendo 512 bytes de datos. La máquina destino responde con paquetes ACK numerados para todos los paquetes de datos.

- El paquete de datos final debe contener menos de 512 bytes de datos para indicar que es el último. Si el tamaño del archivo transferido es un múltiplo exacto de 512 bytes, el origen envía un paquete final que contiene 0 bytes de datos.

8. 2 Implementación TFTP

En una red de gran envergadura siempre tenemos que tener una zona de respaldo, una zona que si cae algún punto de la red no nos quedemos sin servicio.

En la universidad existe un backup de respaldo que esta en los centros de investigación, lo que seria simular otra vez gran parte de la red con la salida a Internet, las conexiones con los otros campus de la universidad Politécnica. Sin embargo vamos a implementar como se realizaría la copia de los ficheros de configuración a un servidor TFTP alojado en esta zona de la red.

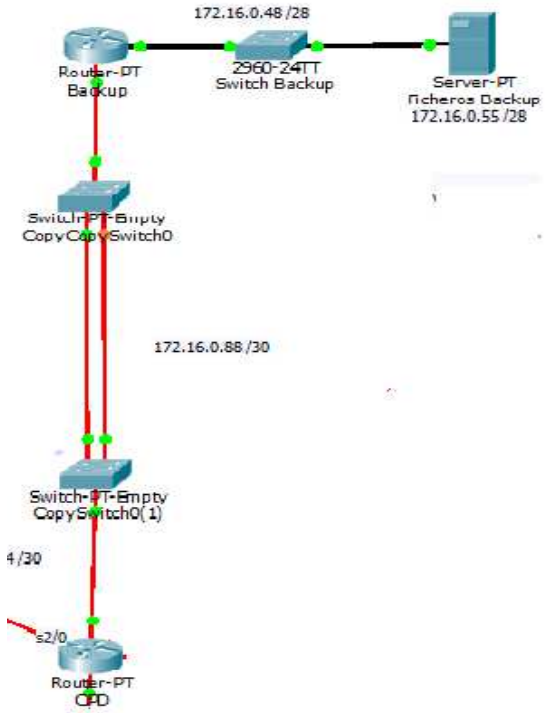


Figura 8.2 – 1, Encale CPD – Backup

1º Vamos al servidor TFTP y los encendemos.

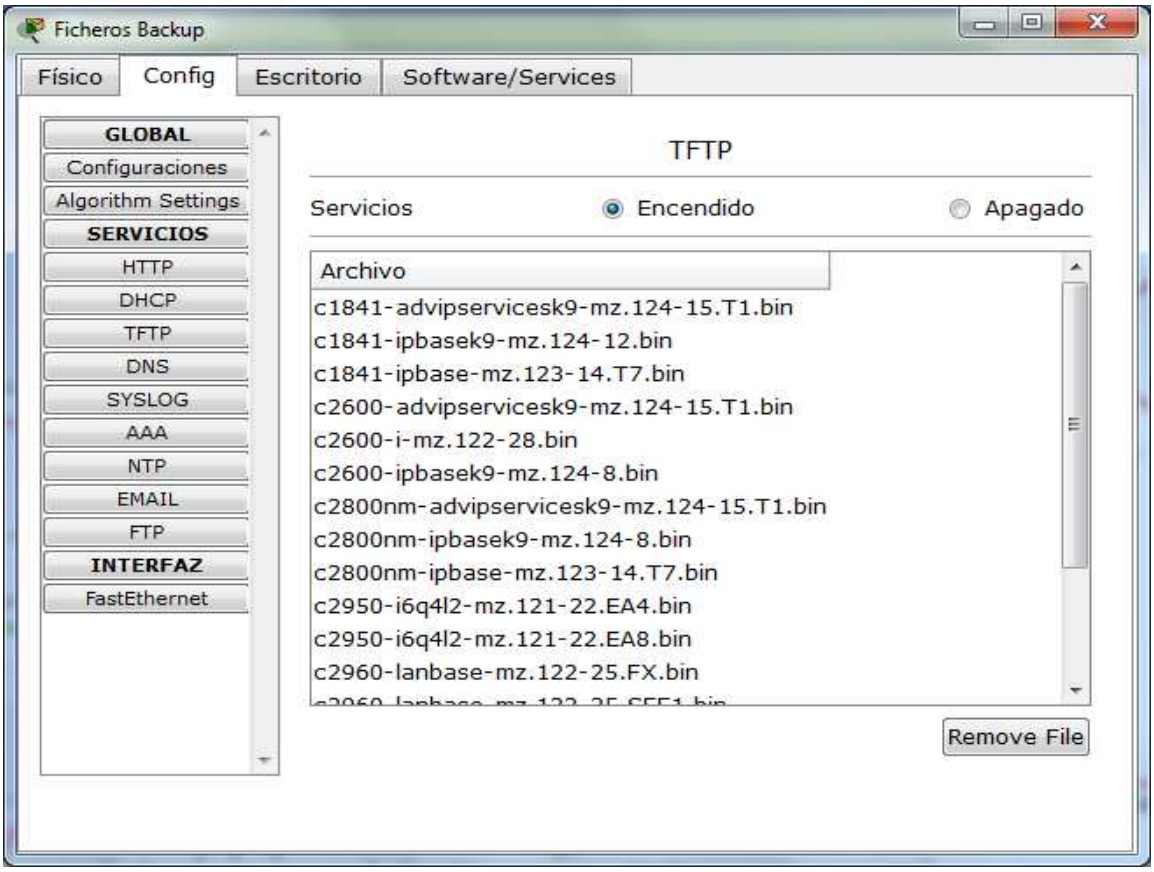


Figura 8.2 – 2 , Configuración servidor TFTP

2º Accedemos a la linea de comandos del router CPD, y lanzamos las siguientes ordenes:

Router#copy st
Router#copy startup-config tftp
Address or name of remote host []? 172.16.0.55
Destination filename [Router-confg]? Configuración CPD

Writing startup-config...!!
[OK - 1300 bytes]

1300 bytes copied in 0.032 secs (40000 bytes/sec)

3º Accedemos al servidor TFTP y veremos nuestro fichero de configuración en la lista de archivos guardado.

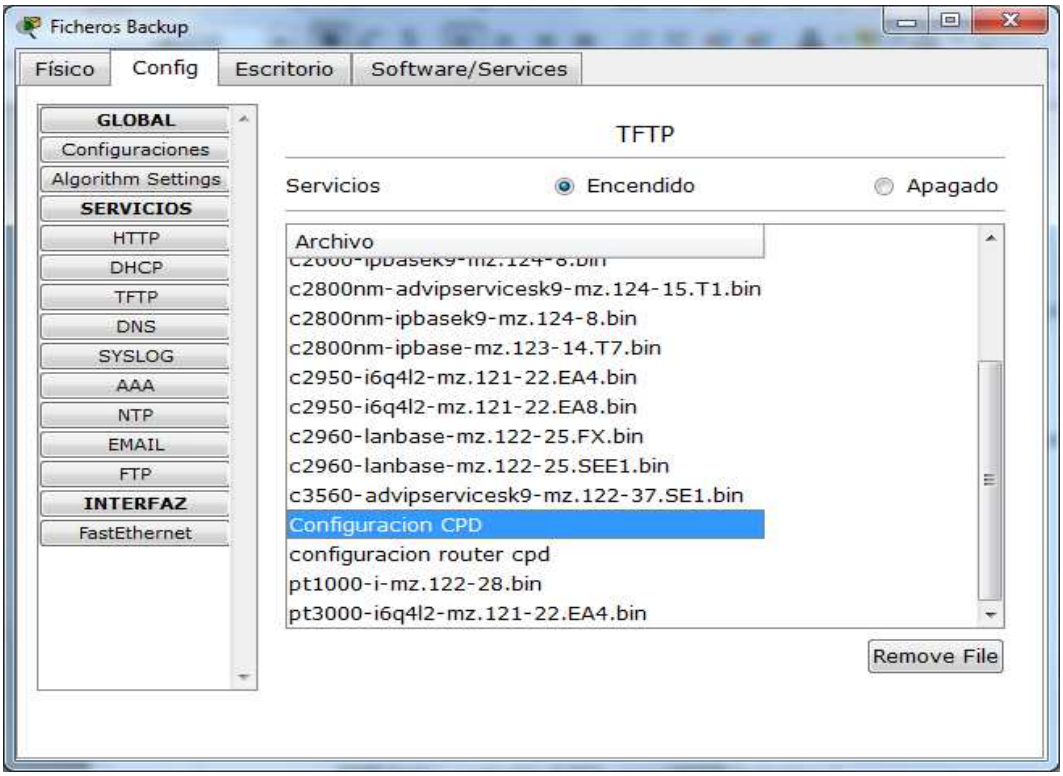


Figura 8.2 – 3 Fichero TFTP

4º Si queremos recuperar la configuración del servidor TFTP accedemos al router en modo configuración y lanzamos las siguientes ordenes.

Router#copy tftp startup-config
Address or name of remote host []? 172.16.0.55
Source filename []? Configuración CPD
Destination filename [startup-config]?

Accessing tftp://172.16.0.55/Configuracion CPD...
Loading Configuracion CPD from 172.16.0.55: !
[OK - 1300 bytes]

1300 bytes copied in 0.02 secs (65000 bytes/sec)

CAPITULO 9

DMZ (zona desmilitarizada)

Zona desmilitarizada (conocida también como DMZ, o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que en general las conexiones desde la DMZ solo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, Web y DNS. Y es precisamente estos servicios alojados en estos servidores los únicos que pueden establecer tráfico de datos entre el DMZ y la red interna, por ejemplo, una conexión de datos entre el servidor web y una base de datos protegida situada en la red interna.

Las conexiones que se realizan desde la red externa hacia la DMZ se controlan generalmente utilizando port address translation (PAT).

Una DMZ se crea a menudo a través de las opciones de configuración del cortafuegos, donde cada red se conecta a un puerto distinto de éste. Esta configuración se llama cortafuegos en trípode (three-legged firewall).

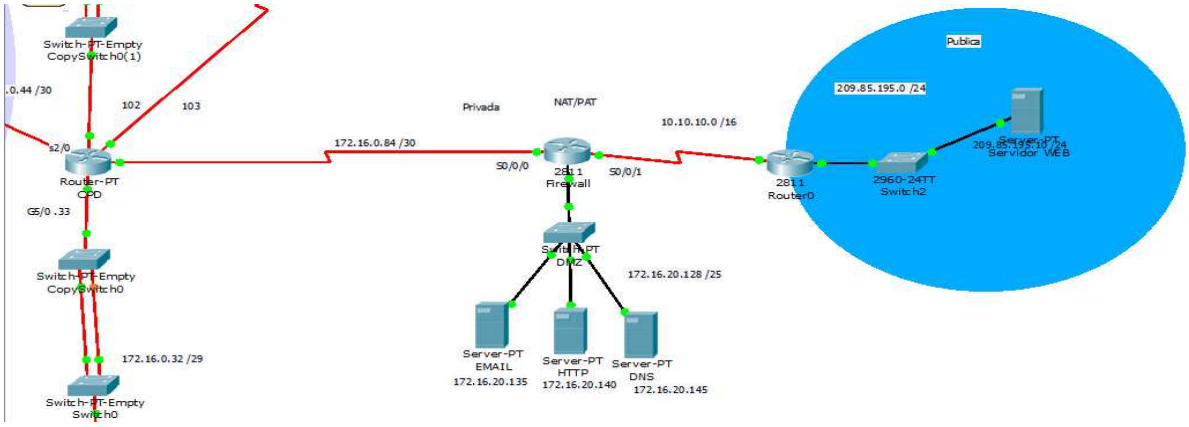


Figura 9.1 – 2, Zona desmilitarizada

Implementación DMZ

9.1 Nat estático

Para la configuración de la DMZ vamos a utilizar un NAT estático para mapear las direcciones Ip's de los tres servidores que se encuentran en al DMZ.

Accedemos al router “Firewall” en modo de configuración y lanzamos los siguientes comandos.

```
Router(config)#ip nat inside source static 192.16.20.135 10.10.10.135
Router(config)#ip nat inside source static 192.16.20.140 10.10.10.140
Router(config)#ip nat inside source static 192.16.20.145 10.10.10.145
Router(config)#int fastEthernet 0/0
Router(config-if)#ip nat inside
Router(config-if)#int serial 0/0/1
Router(config-if)#ip nat outside
```

Ahora tenemos mapeadas las direcciones ip de los servidores, como son servidores en una DMZ les hemos asignado su propia ip publica, mientras que el resto sale al exterior mediante un NAT sobrecargado.

9. 2 Firewall (cortafuegos)

Un cortafuegos (*firewall* en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuegos a una tercera red "DMZ"*, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.*

Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente.

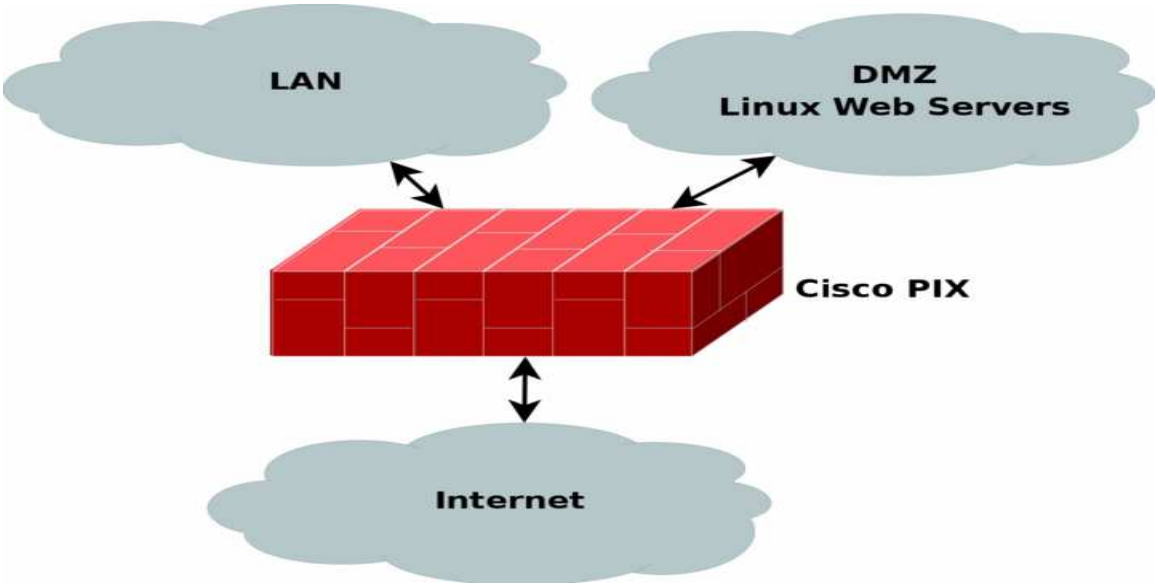


Figura 9.2 – 1 Firewall

9.3 ACL (Listas de acceso)

Una lista de control de acceso o ACL (del inglés, access control list) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición. Sin embargo, también tienen usos adicionales, como por ejemplo, distinguir "tráfico interesante" (tráfico suficientemente importante como para activar o mantener una conexión) en RDSI.

El te responde si tienes permiso de hacerlo o no. Con este enfoque este mismo sistema no solo puede ser utilizado para acceder a lugares si no para cualquier cosa que necesite separarse de personas que pueden y no pueden hacer cosas, por ejemplo: acceder a una página o sección, publicar un comentario, hacer una amistad, enviar un correo,.

En redes informáticas, ACL se refiere a una lista de reglas que detallan puertos de servicio o nombres de dominios (de redes) que están disponibles en un terminal u otro dispositivo de capa de red, cada uno de ellos con una lista de terminales y/o redes que tienen permiso para usar el servicio. Tanto servidores individuales como enrutadores pueden tener ACL de redes. Las listas de control de acceso pueden configurarse generalmente para controlar tráfico entrante y saliente y en este contexto son similares a un cortafuegos.

Funcionamiento de las ACL

Para explicar el funcionamiento utilizaremos el software Cisco IOS.
El orden de las sentencias ACL es importante .

- Cuando el router está decidiendo si se envía o bloquea un paquete, el IOS prueba el paquete, verifica si cumple o no cada sentencia de condición, en el orden en que se crearon las sentencias .
- Una vez que se verifica que existe una coincidencia, no se siguen verificando otras

sentencias de condición .

Por lo tanto, Cisco IOS verifica si los paquetes cumplen cada sentencia de condición de arriba hacia abajo, en orden. Cuando se encuentra una coincidencia, se ejecuta la acción de aceptar o rechazar y ya no se continua comprobando otras ACL.
Por ejemplo, si una ACL permite todo el tráfico y está ubicada en la parte superior de la lista, ya no se verifica ninguna sentencia que esté por debajo.
Si no hay coincidencia con ninguna de las ACL existentes en el extremo de la lista se coloca por defecto una sentencia implícita deny any (denegar cualquiera). Y, aunque la línea deny any no sea visible sí que está ahí y no permitirá que ningún paquete que no coincida con alguna de las ACL anteriores sea aceptado. Se puede añadir de forma explícita por aquello de 'verla' escrita y tener esa tranquilidad.

Proceso completo:

1. Cuando entra una trama a través de una interfaz, el router verifica si la dirección de capa 2 (MAC) concuerda o si es una trama de broadcast.
2. Si se acepta la dirección de la trama, la información de la trama se elimina y el router busca una ACL en la interfaz entrante.
3. Si existe una ACL se comprueba si el paquete cumple las condiciones de la lista.
4. Si el paquete cumple las condiciones, se ejecuta la acción de aceptar o rechazar el paquete.
5. Si se acepta el paquete en la interfaz, se compara con las entradas de la tabla de enrutamiento para determinar la interfaz destino y conmutarlo a aquella interfaz. Luego el router verifica si la interfaz destino tiene una ACL.
6. Si existe una ACL, se compara el paquete con las sentencias de la lista y si el paquete concuerda con una sentencia, se acepta o rechaza el paquete según se indique.
7. Si no hay ACL o se acepta el paquete, el paquete se encapsula en el nuevo protocolo de capa 2 y se envía por la interfaz hacia el dispositivo siguiente.

Hay dos tipos de ACL y utilizan una numeración para identificarse:

- ACL estándar: del 1 al 99
- ACL extendida: del 100 al 199

ACLs estándar: Sintaxis

Las ACL estándar en un router Cisco siempre se crean primero y luego se asignan a una interfaz.
Tienen la configuración siguiente:

Router(config)# access-list numACL permit|deny origen [wild-mask]

El comando de configuración global access-list define una ACL estándar con un número entre 1 y 99.

Se aplican a los interfaces con:

Router (config-if)# ip access-group numACL in|out

- In: tráfico a filtrar que ENTRA por la interfaz del router
- out : tráfico a filtrar que SALE por la interfaz del router.
- wild-mask: indica con 0 el bit a evaluar y con 1 indica que el bit correspondiente se ignora.

Para la creación de ACL estándar en importante:

- Seleccionar y ordenar lógicamente las ACL.
- Seleccionar los protocolos IP que se deben verificar.
- Aplicar ACL a interfaces para el tráfico entrante y saliente.
- Asignar un número exclusivo para cada ACL.

ACLs extendidas: Sintaxis

Las ACL extendidas filtran paquetes IP según:

- Direcciones IP de origen y destino
- Puertos TCP y UDP de origen y destino
- Tipo de protocolo (IP, ICMP, UDP, TCP o número de puerto de protocolo).

Las ACLs extendidas usan un número dentro del intervalo del 100 al 199.

Al final de la sentencia de la ACL extendida se puede especificar, opcionalmente, el número de puerto de protocolo TCP o UDP para el que se aplica la sentencia:

- 20 y 21: datos y programa FTP
- 23: Telnet
- 25: SMTP
- 53: DNS
- 69: TFTP

Definir ACL extendida, sintaxis:

Router(config)#access-list numACL {permit|deny} protocolo fuente [mascara-fuente destino mascara-destino operador operando] [established]

- numACL: Identifica número de lista de acceso utilizando un número dentro del intervalo 100-199
- protocolo: IP, TCP, UDP, ICMP, GRE, IGRP
- fuente | destino: Identificadores de direcciones origen y destino
- mascara-fuente | mascara-destino: Máscaras de wildcard
- operador: lt, gt, eq, neq
- operando: número de puerto
- established: permite que pase el tráfico TCP si el paquete utiliza una conexión establecida.
    - Respecto a los protocolos:
    - Sólo se puede especificar una ACL por protocolo y por interfaz.
    - Si ACL es entrante, se comprueba al recibir el paquete.
    - Si ACL es saliente, se comprueba después de recibir y enrutar el paquete a la interfaz saliente.
    - Se puede nombrar o numerar un protocolo IP.

Asociar ACL a interfaz, sintaxis:

Router(config-if)# ip access-group num_ACL {in | out}

Ubicación de las ACLs

Es muy importante el lugar donde se ubique una ACL ya que influye en la reducción del tráfico innecesario.

El tráfico que será denegado en un destino remoto no debe usar los recursos de la red en el camino hacia ese destino.

La regla es colocar las:

- ACL estándar lo más cerca posible del destino (no especifican direcciones destino).
- ACL extendidas lo más cerca posible del origen del tráfico denegado. Así el tráfico no deseado se filtra sin atravesar la infraestructura de red

Para la simulación no disponemos de un PIX de cisco, por lo que vamos a simular un cortafuegos mediante la administración de listas de control de acceso. Vamos a implementar las reglas básicas para la seguridad de los servidores de la DMZ y de la intranet.

1º Una de las primeras medidas de seguridad que se implantan en una DMZ, es que no se pueda hacer ping a los servidores para evitar un ataque por denegación de servicio. Para evitar eso vamos a crear a siguiente ACL extendida.

Vamos al router “firewall” donde habíamos configurado el NAT previamente y en modo configuración lanzamos la siguiente orden:

Router(config)#access-list 101 deny icmp any 172.16.20.135 0.0.0.127 host-unreachable
Router(config)#access-list 101 deny icmp any 172.16.20.140 0.0.0.127 host-unreachable
Router(config)#access-list 101 deny icmp any 172.16.20.145 0.0.0.127 host-unreachable

Con estas tres primeras reglas denegamos los ping hacia el servidores. Lo que estamos

diciendo es bajo el id= 101 denegamos=deny el protocolo=icmp, origen= cual sea, destino= ip del servidor y el mensaje= host-unreachable

Con las siguientes reglas decimos que permita el paso de trafico bajo esos protocolos y puertos a esas ip's.

Router(config)#access-list 101 permit tcp any 172.16.20.140 0.0.0.127 eq 80
Router(config)#access-list 101 permit tcp any 172.16.20.145 0.0.0.127 eq 53
Router(config)#access-list 101 permit udp any 172.16.20.145 0.0.0.127 eq 53
Router(config)#access-list 101 permit tcp any 172.16.20.140 0.0.0.127 eq 25
Router(config)#access-list 101 permit tcp any 172.16.20.140 0.0.0.127 eq 110

Finalmente asignamos las lista de acceso 101 a la interfaz:

Router(config-if)#int f0/0
Router(config-if)#ip access-group 101 in

ANEXO

Enrutamiento estático

La tabla de enrutamiento contiene la información más importante que usan los routers. Esta tabla proporciona la información que usan los routers para reenviar los paquetes recibidos. Si la información de la tabla de enrutamiento no es correcta, el tráfico se reenviará incorrectamente y posiblemente no llegue al destino. Para que se comprendan las rutas de tráfico, la resolución de problemas y la manipulación del tráfico, es absolutamente necesario que se tengan conocimientos sólidos sobre cómo leer y analizar una tabla de enrutamiento.

El enrutamiento estático proporciona un método que otorga a los ingenieros de redes control absoluto sobre las rutas por las que se transmiten los datos en una internetwork. Para adquirir este control, en lugar de configurar protocolos de enrutamiento dinámico para que creen las tablas de enrutamiento, se crean manualmente. Es importante entender las ventajas y desventajas de la implementación de rutas estáticas, porque se utilizan extensamente en internetworks pequeñas y para establecer la conectividad con proveedores de servicios. Es posible que se crea que el enrutamiento estático es sólo un método antiguo de enrutamiento y que el enrutamiento dinámico es el único método usado en la actualidad. Esto no es así, además, se destaca que escribir una ruta estática en un router no es más que especificar una ruta y un destino en la tabla de enrutamiento, y que los protocolos de enrutamiento hacen lo mismo, sólo que de manera automática. Sólo hay dos maneras de completar una tabla de enrutamiento: manualmente (el administrador agrega rutas estáticas) y automáticamente (por medio de protocolos de enrutamiento dinámico).

Las rutas estáticas por defecto permiten que los administradores reduzcan significativamente el tamaño de las tablas de enrutamiento. Como la tabla de enrutamiento contiene la información más importante para el router, la tabla debe completarse eficazmente. El uso de rutas estáticas por defecto hace que el proceso de enrutamiento sea más eficaz. Concretamente, las tablas de enrutamiento más pequeñas reducen el tiempo de búsqueda de rutas y el uso del procesador, y aceleran el reenvío de paquetes.

Por ultimo vamos a configurar las rutas por defecto y la ruta default para nuestra red.

1º Vamos a configurar las rutas por defecto para ir al campus de Gandia y Alcoy. Accedemos al modo de configuración del router “CPD” y lanzamos los siguientes comandos

Router(config)#ip route 192.168.1.0 255.255.255.0 10.0.0.2 → Ruta Gandia
Router(config)#ip route 192.168.2.0 255.255.255.0 10.0.0.10 → Ruta Alcoy

Lo que le decimos es que para ir a la **red** 192.168.1.0 con **mascara** 255.255.0.0 saldrá por la ultima interfaz directamente conectada, que es la serial 10.10.10.2, para la ruta hacia Gandia y realizamos lo mismo para la ruta hacia Alcoy.

2º Vamos a configurar la ruta default, entrando en modo configuración del router firewall, añadimos la siguiente ruta:

Router(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2

Lo que queremos decir con esto es, para ir a cualquier red 0.0.0.0 con mascara-destino la que sea 0.0.0.0 salimos por la ultima interfaz conectada a la parte privada 10.10.10.2

SUBNETING

Enalces

listas /30 REDES 4 DIRECCIONES 2 HOSTS

Dirección de Red	Rango de Host	Dirección Broadcast	Enlace
172.16.0.32	172.16.0.33 to 172.16.0.34	172.16.0.35	CPD-ETSINF
172.16.0.36	172.16.0.37 to 172.16.0.38	172.16.0.39	
172.16.0.40	172.16.0.41 to 172.16.0.42	172.16.0.43	
172.16.0.44	172.16.0.45 to 172.16.0.46	172.16.0.47	CPD-CAPD2
172.16.0.48	172.16.0.49 to 172.16.0.50	172.16.0.51	BIBLIOTECA-CPD2
172.16.0.52	172.16.0.53 to 172.16.0.54	172.16.0.55	ARQUITECTUR-BIBLIOTECA
172.16.0.56	172.16.0.57 to 172.16.0.58	172.16.0.59	ARQUITECTURA-CAMINOS
172.16.0.60	172.16.0.61 to 172.16.0.62	172.16.0.63	INDUSTRI-ARQUITCTURA
172.16.0.64	172.16.0.65 to 172.16.0.66	172.16.0.67	INDUSTRI-INSDUSTRI2
172.16.0.68	172.16.0.69 to 172.16.0.70	172.16.0.71	INDSUTRI-CASA ALUMNO
172.16.0.72	172.16.0.73 to 172.16.0.74	172.16.0.75	CPD2 -CASA ALUMNO
172.16.0.76	172.16.0.77 to 172.16.0.78	172.16.0.79	CAMINOS-CPD2
172.16.0.80	172.16.0.81 to 172.16.0.82	172.16.0.83	NDUSTRI2-CAMINOS
172.16.0.84	172.16.0.85 to 172.16.0.86	172.16.0.87	CPD-FIREWALL
172.16.0.88	172.16.0.89 to 172.16.0.90	172.16.0.91	CPD- BACKUP
172.16.0.92	172.16.0.93 to 172.16.0.94	172.16.0.95	EDIFI-EDIFI2
172.16.0.96	172.16.0.97 to 172.16.0.98	172.16.0.99	RECTORA-EDIFI2
172.16.0.100	172.16.0.101 to 172.16.0.102	172.16.0.103	BELLAS ARTES - ETSINF
172.16.0.104	172.16.0.105 to 172.16.0.106	172.16.0.107	
172.16.0.108	172.16.0.109 to 172.16.0.110	172.16.0.111	
172.16.0.112	172.16.0.113 to 172.16.0.114	172.16.0.115	

Servidores /25

Dirección de Red	**Rango de Hosts**	**Dirección de Broadcast**	**Enlace**
172.16.20.0	172.16.20.1 to 172.16.20.126	172.16.20.127	SERVIDORES CPD2
172.16.20.128	172.16.20.129 to 172.16.20.254	172.16.20.255	DMZ
172.16.20.0	172.16.20.1 to 172.16.23.254	172.16.23.255	SERVIDORES IN INTRANET

llstas donde caben 12 host 14 direcciones por subred

e la 172.16.0.0 Red con Máscara de Red 255.255.255.240 /28

Dirección de Red	Rango de Hosts	Dirección de Broadcast	Enlace
172.16.0.0	172.16.0.1 to 172.16.0.14	172.16.0.15	MALLA RIP
172.16.0.16	172.16.0.17 to 172.16.0.30	172.16.0.31	RED SERVIDOR DHCP
172.16.0.32	172.16.0.33 to 172.16.0.46	172.16.0.47	TRONCALES DE FIBRA1
172.16.0.48	172.16.0.49 to 172.16.0.62	172.16.0.63	BACKUP
172.16.0.64	172.16.0.65 to 172.16.0.78	172.16.0.79	
172.16.0.80	172.16.0.81 to 172.16.0.94	172.16.0.95	
172.16.0.96	172.16.0.97 to 172.16.0.110	172.16.0.111	
172.16.0.112	172.16.0.113 to 172.16.0.126	172.16.0.127	
172.16.0.128	172.16.0.129 to 172.16.0.142	172.16.0.143	
172.16.0.144	172.16.0.145 to 172.16.0.158	172.16.0.159	

De la 172.16.0.0 Red con Máscara de Red 255.255.252.0 /22

Dirección de de Hosts	Rango de Hosts	Dirección de Broadcast	Enlace
172.16.0.0	172.16.0.1 to 172.16.3.254	172.16.3.255	
172.16.4.0	172.16.4.1 to 172.16.7.254	172.16.7.255	
172.16.8.0	172.16.8.1 to 172.16.11.254	172.16.11.255	VLAN ALUMNOS
172.16.12.0	172.16.12.1 to 172.16.15.254	172.16.15.255	VLAN PROFESORES
172.16.16.0	172.16.16.1 to 172.16.19.254	172.16.19.255	ADMINISTRACIÓN

172.16.20.0	172.16.20.1 to 172.16.23.254	172.16.23.255 --> pero con /25	
172.16.24.0	172.16.24.1 to 172.16.27.254	172.16.27.255	WIRELESS
172.16.28.0	172.16.28.1 to 172.16.31.254	172.16.31.255	
172.16.32.0	172.16.32.1 to 172.16.35.254	172.16.35.255	
172.16.36.0	172.16.36.1 to 172.16.39.254	172.16.39.255	

CAMPUS MASCARA 255.255.255.0 /24

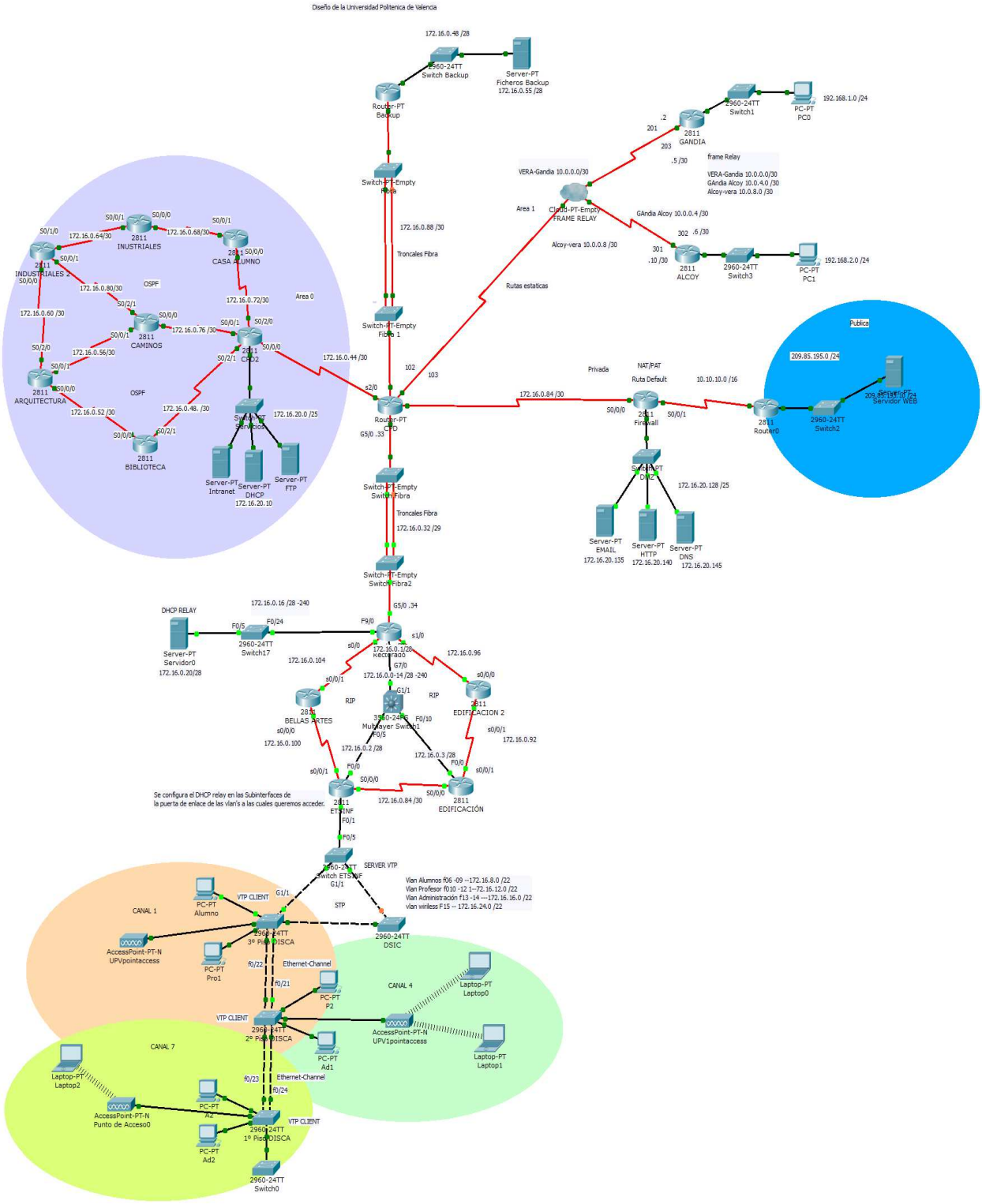
Dirección de Hosts	de	Rango de Hosts	Dirección de Broadcast	Enlace
192.168.1.0		182.168.1.1 to 192.168.1.254	192.168.1.255	Gandia
192.168.2.0		182.168.2.1 to 192.168.2.254	192.168.2.255	Alcoy

INTERNET MASCARA 255.255.0.0 /16

Dirección de Hosts	de	Rango de Hosts	Dirección de Broadcast	Enlace
10.10.10.0		10.10.10.1 – 10.10.254.254	10.10.10.255	Internet

FRAME RELAY MASCARA 255.255.255.252 /30

Dirección de Hosts	de	Rango de Hosts	Dirección de Broadcast	Enlace
10.0.0.0		10.0.0.1 – 10.0.0.2	10.0.0.3	VERA-GANDIA
10.0.4.0		10.0.4.1 – 10.0.4.2	10.0.4.3	GANDIA-ALCOY
10.0.8.0		10.0.8.1 – 10.0.8.2	10.10.8.3	ALCOY -VERA


Diseño de la Universidad Politecnica de Valencia
172.16.0.48 /28
2960-24TT
Switch Backup
Server-PT
Ficheros Backup
172.16.0.55 /28
Router-PT
Backup
Switch-PT-Empty
Fibra
172.16.0.88 /30
Troncales Fibra
Switch-PT-Empty
Fibra 1
172.16.0.44 /30
102
103
Rutas estaticas
Area 0
OSPF
172.16.0.72/30
172.16.0.76 /30
172.16.0.56/30
172.16.0.60 /30
172.16.0.80/30
172.16.0.64/30
172.16.0.68/30
172.16.0.52 /30
172.16.0.48. /30
2811
INUSTRIALES
2811
INDUSTRIALES 2
2811
CASA ALUMNO
2811
CAMINOS
2811
CPD2
2811
ARQUITECTURA
2811
BIBLIOTECA
Switch-PT
Servicios
172.16.20.0 /25
Server-PT
Intranet
Server-PT
DHCP
172.16.20.10
Server-PT
FTP
Router-PT
CPD
s2/0
G5/0 .33
172.16.0.84 /30
Switch-PT-Empty
Switch Fibra
Troncales Fibra
172.16.0.32 /29
Switch-PT-Empty
Switch Fibra2
G5/0 .34
Area 1
Cloud-PT-Empty
FRAME RELAY
VERA-Gandia 10.0.0.0/30
GAndia Alcoy 10.0.4 /30
Alcoy-vera 10.0.8 /30
frame Relay
VERA-Gandia 10.0.0.0/30
GAndia Alcoy 10.0.4.0 /30
Alcoy-vera 10.0.8.0 /30
2811
GANDIA
2960-24TT
Switch1
PC-PT
PC0
192.168.1.0 /24
.2
201
203
.5 /30
2811
ALCOY
2960-24TT
Switch3
PC-PT
PC1
192.168.2.0 /24
302
.6 /30
301
.10 /30
Privada
NAT/PAT
Ruta Default
10.10.10.0 /16
172.16.0.84 /30
2811
Firewall
Switch-PT
DMZ
172.16.20.128 /25
Server-PT
EMAIL
172.16.20.135
Server-PT
HTTP
172.16.20.140
Server-PT
DNS
172.16.20.145
2811
Router0
2960-24TT
Switch2
Publica
209.85.195.0 /24
Server-PT
Servidor WEB
DHCP RELAY
Server-PT
Servidor0
172.16.0.20/28
172.16.0.16 /28 -240
2960-24TT
Switch17
F0/5
F0/24
F9/0
s1/0
s0/0
172.16.0.1/28
Kecarabo
G7/0
172.16.0.96
172.16.0.104
172.16.0.0-14 /28 -240
s0/0/1
s0/0/0
RIP
2811
BELLAS ARTES
3560-24PS
Multilayer Switch1
G1/1
F0/10
F0/5
2811
EDIFICACION 2
s0/0/0
172.16.0.100
s0/0/1
172.16.0.92
172.16.0.2 /28
172.16.0.3 /28
F0/0
F0/1
s0/0/1
2811
ETSINF
S0/0/0
172.16.0.84 /30
2811
EDIFICACIÓN
Se configura el DHCP relay en las Subinterfaces de
la puerta de enlace de las vlan's a las cuales queremos acceder.
F0/1
F0/5
2960-24TT
Switch ETSINF
SERVER VTP
G1/1
Vlan Alumnos f06 -09 --172.16.8.0 /22
Vlan Profesor f010 -12 1--72.16.12.0 /22
Vlan Administración f13 -14 ---172.16.16.0 /22
Vlan wirless F15 -- 172.16.24.0 /22
CANAL 1
PC-PT
Alumno
VTP CLIENT
G1/1
STP
2960-24TT
3º Piso DISCA
2960-24TT
DSIC
AccessPoint-PT-N
UPVpointaccess
PC-PT
Pro1
f0/22
Ethernet-Channel
f0/21
PC-PT
P2
CANAL 4
Laptop-PT
Laptop0
VTP CLIENT
2960-24TT
2º Piso DISCA
AccessPoint-PT-N
UPV1pointaccess
Laptop-PT
Laptop1
PC-PT
Ad1
CANAL 7
Laptop-PT
Laptop2
f0/23
Ethernet-Channel
f0/24
PC-PT
P2
AccessPoint-PT-N
Punto de Acceso0
VTP CLIENT
2960-24TT
1º Piso DISCA
PC-PT
Ad2
2960-24TT
Switch0

BIBLIOGRAFÍA

- REDES CISCO. GUÍA DE ESTUDIO PARA LA CERTIFICACIÓN CCNA ROUTING Y SWITCHING ARIGANELLO, ERNESTO ,AÑO DE EDICIÓN2014, ISBN978-84-9964-272-7

- REDES CISCO. GUIA DE ESTUDIO PARA LA CERTIFICACION CCNP COMPRENDE LOS EXAMENES 642-902 ROUTE - 642-813 SWITCH - 642-832 TSHOOT SBN978-84-9964-035-8

- CONCEPTOS Y PROTOCOLO DE ENRUTAMIENTO: GUIA DE PRACTICAS DE CCNNA EXPLORATION ALLAN G. JOHNSON , PRENTICE-HALL, 2009 ISBN 9788483224762
- LAN INALAMBRICA Y CONMUTADA (GUIA DE PRACTICAS Y LABORATORIOS EXP LORATION) (INCLUYE CD-ROM CON ACTIVIDADES PACKET TRACER Y ARCHI IVOS DE INFORMACION SOBRE NUEVAS TECNOLOGIAS) (En papel)ALLAN G. JOHNSON , PRENTICE-HALL, 2009 ISBN 9788483224779

- CONCEPTOS Y PROTOCOLOS DE ENRUTAMIENTO . CCNA EXPLORATION EDITORIAL: PEARSON. AUTOR: CISCO, AÑO: 2009, ISBN 8483224720