DISEÑO, ADMINISTRACIÓN Y SEGURIDAD DE REDES

Prácticas guiadas de laboratorio

UVa

Universidad de Valladolid

Autores: Juan A. Muñoz Cristóbal

Departamento de Informática

Universidad de Valladolid

Julio 2024

Versión 1.0

Con el apoyo de VirtUva

Proyecto de Innovación Docente 2023-24

PRESENTACIÓN

Los presentes guiones de trabajo se corresponden con las prácticas guiadas de laboratorio de la asignatura Diseño, Administración y Seguridad de Redes, del Grado en Ingeniería Informática de la UVa. Ésta es una asignatura de nivel medio de redes, en donde el estudiantado profundiza en los conocimientos necesarios para poder diseñar y configurar una red segura. En las prácticas se utiliza un simulador de redes (Cisco Packet Tracer). Las prácticas guiadas sirven de entrenamiento para la realización de un proyecto complejo que tiene que realizar el estudiantado en grupos. Las prácticas guiadas tienen cierta complejidad, por lo que una dinámica adecuada es que sea el profesor el que va realizando la configuración, y el alumnado le vaya siguiendo. Para poder evaluar la actividad del alumnado, en cada práctica puede generarse un instrumento de evaluación, como un cuestionario, o un documento en el que cada estudiante va incorporando las capturas que solicita el profesor.

El motivo de la redacción de este documento es el de ofrecer un material de apoyo a los alumnos de la asignatura de Diseño, Administración y Seguridad de Redes, así como que pueda servir se ayuda en otras asignaturas de la UVa o de otras organizaciones educativas.

UVa

Tabla de contenido

1. Listas de acceso (ACLs)

1.1 Objetivo

El objetivo de esta práctica es aprender a configurar listas de acceso (ACL) en routers Cisco para proteger una red.

1.2 Competencias

Tras la finalización de la práctica deberían haberse adquirido las siguientes competencias:

- Conocer los filtros básicos que son necesarios en el router de acceso a internet de una red sencilla para protegerla.
- Saber cómo configurar listas de acceso (ACL) en routers Cisco.

1.3 Enlaces de interés

- Chapter 9 – Access Lists
- MONOGRÁFICO: Listas de control de acceso (ACL) - Utilización de ACLs en routers
- Configure Commonly Used IP ACLs

1.4 Breve presentación de las ACLs[1]

Las ACL son listas de condiciones que se aplican al tráfico que viaja a través de la interfaz del router. Estas listas pueden aplicarse luego para múltiples funcionalidades. La más conocida es la que aplica la lista en una interfaz en sentido entrante o saliente, para filtrar el tráfico, permitiéndolo o denegándolo, a modo de firewall. En este caso, estas listas le informan al router qué tipo de paquetes aceptar o rechazar. La aceptación y rechazo se pueden basar en ciertas condiciones específicas.

Las ACL permiten la administración del tráfico y aseguran el acceso hacia y desde una red. Las ACL filtran el tráfico de red, controlando si los paquetes enrutados se envían o se bloquean en las interfaces del router. El router examina cada paquete y lo enviará o lo descartará, según las condiciones especificadas en la ACL. Algunos de los puntos de decisión de ACL son direcciones origen y destino, protocolos y números de puerto de capa superior.

Estas son las razones principales para crear las ACL:

- Limitar el tráfico de red y mejorar el rendimiento de la red. Al restringir el tráfico de

[1] Extraído del Cisco Networking Academy Program CCNA 2

video, por ejemplo, las ACL pueden reducir ampliamente la carga de la red y en consecuencia mejorar el rendimiento de la misma.

- Brindar control de flujo de tráfico. Las ACL pueden restringir el envío de las actualizaciones de enrutamiento. Si no se necesitan actualizaciones debido a las condiciones de la red, se preserva el ancho de banda.
- Proporcionar un nivel básico de seguridad para el acceso a la red. Por ejemplo, las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro acceda a la misma área. Por ejemplo, al Host A se le permite el acceso a la red de Recursos Humanos, y al Host B se le niega el acceso a dicha red.
- Previa decisión de los tipos de tráfico se envían o bloquean en las interfaces del router, permitir que se enrute el tráfico de correo electrónico, pero bloquear todo el tráfico de telnet.
- Permitir que un administrador controle a cuáles áreas de la red puede acceder un cliente.
- Analizar ciertos hosts para permitir o denegar acceso a partes de una red.
- Otorgar o denegar permiso a los usuarios para acceder a ciertos tipos de archivos, tales como FTP o HTTP.

Si las ACL no están configuradas en el router, todos los paquetes que pasen a través del router tendrán acceso a todas las partes de la red.

El orden en el que se ubican las sentencias (o *statements*) de la ACL es importante. El software Cisco IOS verifica si los paquetes cumplen cada sentencia de condición, en orden, desde la parte superior de la lista hacia abajo. Una vez que se encuentra una coincidencia, se lleva a cabo la acción de aceptar o rechazar y no se verifican otras sentencias ACL. Si una sentencia de condición que permite todo el tráfico está ubicada en la parte superior de la lista, no se verifica ninguna sentencia que esté por debajo.

Si se requieren más cantidad de sentencias de condición en una lista de acceso, se debe borrar y volver a crear toda la ACL con las nuevas sentencias de condición.

A manera de revisión, las sentencias de la ACL operan en orden secuencial lógico. Si se cumple una condición, el paquete se permite o deniega, y el resto de las sentencias de la ACL no se verifican. Si todas las sentencias ACL no tienen coincidencias, se coloca una sentencia implícita que dice **deny any** (denegar cualquiera) en el extremo de la lista por defecto. Aunque la línea **deny any** no sea visible como última línea de una ACL, está ahí y no permitirá que ningún paquete que no coincida con las líneas anteriores de la ACL sea aceptada. Cuando esté aprendiendo por primera vez cómo crear una ACL, es una buena práctica agregar el **deny any** al final de las ACL para reforzar la presencia dinámica de la prohibición implícita **deny**.

En TCP/IP, las ACL se asignan a una o más interfaces y pueden filtrar el tráfico entrante o saliente.

Es necesario utilizar estas reglas básicas a la hora de crear y aplicar las listas de acceso.

1. Se deben aplicar las listas de acceso estándar que se encuentran lo más cerca posible del destino.
2. Se deben aplicar las listas de acceso extendidas que se encuentran lo más cerca posible del origen.
3. Utilice la referencia de la interfaz entrante y saliente como si estuviera mirando el puerto

desde adentro del router.

4. Las sentencias se procesan de forma secuencial desde el principio de la lista hasta el final hasta que se encuentre una concordancia, si no se encuentra ninguna, se rechaza el paquete.
5. Hay un **deny any** (denegar cualquiera) implícito al final de todas las listas de acceso. Esto no aparece en la lista de configuración.
6. Las entradas de la lista de acceso deben realizar un filtro desde lo particular a lo general. Primero se deben denegar hosts específicos y por último los grupos o filtros generales.
7. Primero se examina la condición de concordancia. El permiso o rechazo se examina SÓLO si la concordancia es cierta.
8. Nunca trabaje con una lista de acceso que se utiliza de forma activa.
9. Utilice el editor de texto para crear comentarios que describan la lógica, luego complete las sentencias que realizan esa lógica.
10. Siempre, las líneas nuevas se agregan al final de la lista de acceso. El comando **no access-list** elimina toda la lista. No es posible agregar y quitar líneas de manera selectiva en las ACL numeradas.
11. Una lista de acceso IP envía un mensaje ICMP llamado de host fuera de alcance al emisor del paquete rechazado y descarta el paquete en la papelera de bits.
12. Se debe tener cuidado cuando se descarta una lista de acceso. Si la lista de acceso se aplica a una interfaz de producción y se la elimina, según sea la versión de IOS, puede haber una **deny any** (denegar cualquiera) por defecto aplicada a la interfaz, y se detiene todo el tráfico.
13. Los filtros salientes no afectan al tráfico que se origina en el router local.

1.4.1 Sintaxis

La sintaxis completa del comando *ACL estándar* es:

```
Router(config)# access-list access-list-number {deny | permit | remark} source [source-wildcard] [log]
```

Las *ACL extendidas* se utilizan con más frecuencia que las ACL estándar porque ofrecen un mayor control. Las ACL extendidas verifican las direcciones de paquetes de origen y destino, y también los protocolos, números de puerto, etc.

```
Router(config)# access-list access-list-number {deny | permit | remark} { protocolo tpc/udp/icmp/... } source [source-wildcard] [destination [destination-wildcard]] [ { established | eq puerto | tipo_mensaje } ] [log]
```

1.4.2 Máscara de wildcard

Las máscaras de *wildcard* se usan en lugar de las direcciones de source o destination. Usan unos y ceros binarios para filtrar direcciones IP individuales o en grupos, permitiendo o rechazando el acceso a recursos según el valor de las mismas. La única similitud entre la máscara wildcard y la de subred es que ambas tienen 32 bits de longitud y se componen de

unos y ceros. Un **0** significa que se deje pasar el valor para verificarlo. Los **1** significan impedir que se compare el valor (lo que en la práctica equivale a utilizar un comodín "**?**").

Hay dos palabras clave especiales que se utilizan en las ACL, las opciones **any** y **host**, que se utilizan en lugar de dirección y máscara de origen y/o destino. Para explicarlo de forma sencilla, la opción **any** reemplaza la dirección IP con 0.0.0.0 y la máscara *wildcard* por 255.255.255.255. Esta opción admite cualquier dirección con la que se la compare. En la opción **host** la máscara es 0.0.0.0. Esta máscara necesita que se indiquen todos los bits de la dirección de la máquina y por tanto admite paquetes sólo de esa dirección IP.

1.4.3 Aplicación de ACLs

El comando **ip access-group** enlaza una ACL extendida existente a una interfaz. Recuerde que sólo se permiten dos ACL por interfaz y protocolo, una para los paquetes de entrada, y otra para los de salida. El formato del comando es:

```
Router(config-if)#ip access-group access-list-number {in | out}
```

***Atención**: Una ACL que contiene sentencias ACL numeradas no puede ser alterada. Se debe borrar utilizando el comando* **no access-list** *list-number* y entonces proceder a recrearla.

1.4.4 Mostrar la información sobre las ACL

El comando **show ip interface** muestra información de la interfaz IP e indica si se ha establecido alguna ACL. El comando **show access-lists** muestra el contenido de todas las ACL en el router. Para ver una lista específica, agregue el nombre o número ACL como opción a este comando. El comando **show running-config** también revela las listas de acceso en el router y la información de asignación de interfaz.

1.4.5 Ejemplo de configuración

1. Configuración de ACL

```
Router> enable
Router# configure terminal
Router(config)# access-list 101 permit ip 10.10.10.0 0.0.0.255 any
Router(config)# access-list 101 permit ip 10.10.20.0 0.0.0.255 any
```

2. Aplicación de ACL en interfaz, para tráfico entrante en la interfaz

```
Router(config)# interface fastEthernet 0/1
Router(config-if)# ip access-group 101 in
```

1.4.6 Ejemplos de ACLs típicas

- Permitir respuestas a peticiones TCP (paquetes TCP de sesiones establecidas):

```
access-list 101 permit tcp any [source_network] [wildcard_mask]
established
```

- Permitir pings desde una red:

```
access-list 101 permit icmp [source_network] [wildcard_mask] any
echo
```

- Permitir pings desde una red hacia un host destino:

```
access-list 101 permit icmp [source_network] [wildcard_mask] host
[destination_IP]
```

- Permitir paquetes ICMP echo-reply (respuestas a pings) con destino una red concreta:

```
access-list 101 permit icmp any [destination_network]
[wildcard_mask] echo-reply
```

- Permitir rechazos ICMP (rechazos de pings) con destino una red concreta:

```
access-list 101 permit icmp any [destination_network]
[wildcard_mask] unreachable
```

- Permitir paquetes originados en una red concreta, usando una ACL estándar:

```
access-list 1 permit [source_network] [wildcard_mask]
```

- Permitir paquetes originados en una red concreta, usando una ACL extendida:

```
access-list 101 permit ip [source_network] [wildcard_mask] any
```

- Permitir paquetes HTTP a un host destino:

```
access-list 101 permit tcp any host [destination_IP] eq www
```

- Permitir respuestas HTTP desde un host:

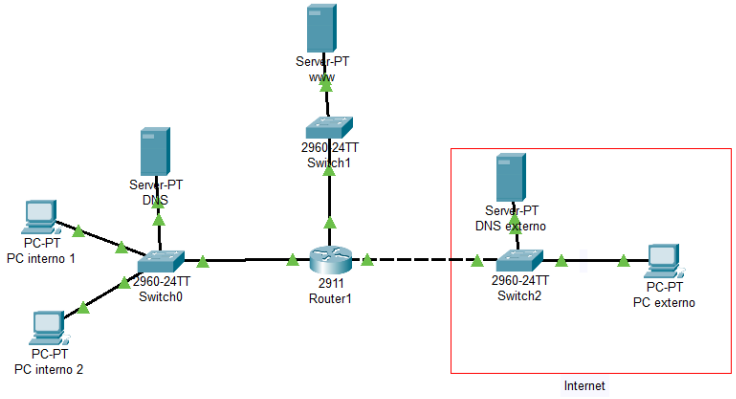
```
access-list 101 permit tcp host [source_IP] eq www any established
```

- Denegar tráfico desde una red:

```
access-list 101 deny ip [source_network] [wildcard_mask] any
```

1.5 Configuración de ACLs para protección de una red sencilla con DMZ

Un posible uso de las ACL podría ser para proteger una red con un servidor web expuesto a internet. En la siguiente imagen puede verse un ejemplo de dicha red, y un posible listado de ACLs que permitirían proteger la red, mientras permitirían acceso al servidor web. La web está simplificada para centrar el ejemplo en ACLs, ya que en la red interna se usa direccionamiento privado, que no debería salir hacia internet. Con el fichero de packet tracer proporcionado, que contiene la red sin protección, esta práctica consiste en configurar ACLs que implementen en el router los filtros indicados, de tal forma que se permita el funcionamiento normal de la red, protegiendo accesos no deseados.



FILTRO RED INTERNA:

1. Sólo se permite salir hacia red interna:
- Respuestas de peticiones TCP originadas en red interna
- ICMP echo reply
- ICMP unreachable

2. Sólo se permite entrar desde la red interna tráfico con IP origen de la red interna

FILTRO RED WEB:

3. Sólo se permite salir hacia red Web:
- Tráfico HTTP al servidor Web
- ICMP con origen red interna

4. Sólo se permite entrar desde red Web tráfico con IP origen de la red Web

FILTRO INTERNET:

5. Sólo se permite salir hacia internet:
- Tráfico con origen la red interna
- Respuestas procedentes del servidor web de peticiones web

6. Sólo se permite entrar desde internet:
- Se deniega cualquier tráfico con origen IPs de red interna, IP servidor Web, 127.0.0.0/8
- Se permite peticiones Web al servidor Web
- Se permite respuestas TCP hacia red interna
- Se permite ICMP echo reply hacia red interna
- Se permite ICMP unreachable hacia red interna

2. DNS y NAT

2.1 Objetivo

El objetivo de esta práctica es aprender nociones básicas de DNS y NAT y a configurar NAT en un router Cisco.

2.2 Competencias

Tras la finalización de la práctica deberían haberse adquirido las siguientes competencias:

- Conocer qué es y para qué sirve un DNS.
- Conocer qué son los tipos de registros DNS A y NS y para qué se usan en una red.
- Saber qué es y para qué sirve la traducción de nombres de red (NAT).
- Saber cómo configurar NAT estática y dinámica en un router Cisco

2.3 Enlaces de interés

- Capítulo 10 CCNA freestudy guide en la carpeta CCNA de los recursos de la asignatura (ojo, hay un error en los comandos de NAT estático, la config correcta es "ip nat **inside** source static <ip_a_traducir> <ip_traducida> ...")
- How Network Address Translation Works
- Explicación genérica del funcionamiento de DNS, y recomendaciones de diseño
- White paper con propuesta de diseño de DNS para organización

2.4 Domain Name System (DNS)

DNS se refiere a toda la infraestructura que existe en Internet para gestionar los nombres de dominio. Los nombres de dominio, o dominios a secas, son nombres asociados a las direcciones IP que facilitan el manejo de las mismas. Los dominios pueden tener subdominios, que permiten agrupar conjuntos de máquinas de forma más conveniente. El nombre de dominio es usado junto con el nombre del host para crear lo que se denomina *fully qualified domain name* (FQDN). Éste está formado por el nombre del host, un punto, y el nombre del dominio. Por ejemplo, **subred.mired.es** es un subdominio del dominio **mired.es**, dentro del cual puede encontrarse la máquina **xyz.subred.mired.es** con la dirección IP **123.123.123.123** .

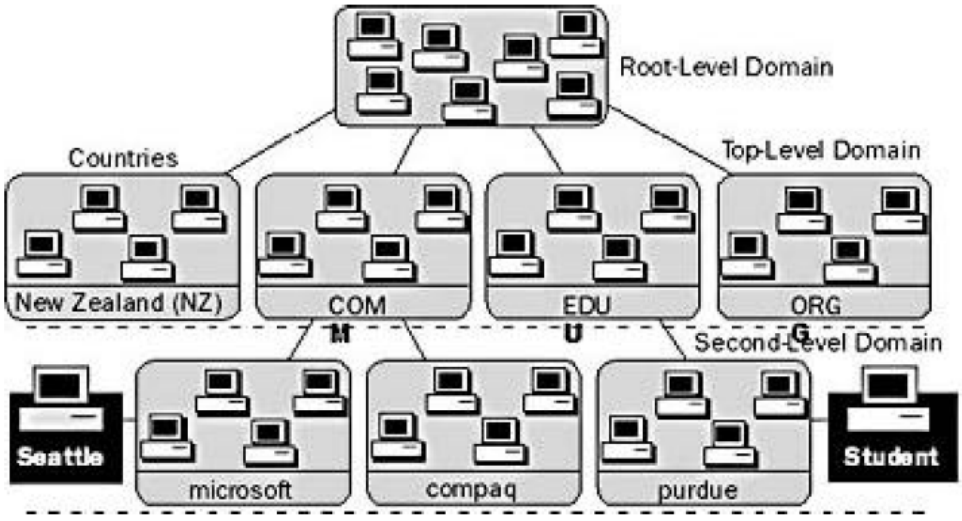
Aunque la configuración del servicio DNS está fuera del alcance de la asignatura, es conveniente comprender el funcionamiento básico para poder ubicar correctamente los servidores DNS. DNS actúa de algún modo como las agendas de los teléfonos modernos, en los que en lugar de teclear el número de abonado al que se desea llamar, se elige un nombre y

la agenda hace la traducción y los pasos necesarios para llamar a dicho contacto utilizando su número de teléfono.

Además de este servicio básico, DNS proporciona otros como:

- **alias de host**: lo que permite que una misma máquina pueda ser conocida por varios nombres.
- **alias de servidor de correo**: lo que permite averiguar la dirección del servidor de correo para un dominio.
- **distribución de carga**: lo que permite que varias direcciones IP estén asociadas con el mismo nombre de máquina.

DNS está compuesto por una base de datos distribuida compuesta por una **jerarquía de servidores** de nombres y por un **protocolo de consulta** a esa base de datos. La siguiente imagen ilustra la jerarquía de DNS.



Fuente: Microsoft Corporation (2000). MCSE Training Kit, Microsoft Windows 2000 Network Infrastructure Administration. Microsoft Press. ISBN 1-57231-904-6

Como puede verse en la figura, DNS se agrupa en distintos niveles. El nivel raíz, root, guarda la base de datos de servidores DNS autoritativos de dominios del siguiente nivel, llamado top-level (nivel más alto). Los dominios top-level pueden contener dominios de segundo nivel y hosts. Normalmente a partir del segundo nivel los dominios suelen denominarse sencillamente subdominios.

2.4.1 Espacios de nombres

En una organización tendremos probablemente un espacio de nombres que expondremos al exterior, y un espacio de nombres de uso únicamente interno. El espacio de nombres externo es aquel que usarán usuarios externos a la red para acceder a los servicios públicos de la red, por ejemplo, a un servidor Web accesible desde el exterior. El espacio de nombres interno es

aquel que usarán los usuarios internos de la red para acceder a servicios internos, como por ejemplo para obtener la dirección IP de una impresora.
Generalmente usaremos DNS distintos para cada uno de estos espacios de nombres. Cada uno de estos DNSs necesitará redundancia si los requisitos de la red así lo requieren.

Por otro lado, los usuarios internos de la red usarán a su vez nombres externos (por ejemplo, google.com). Para ello usarán DNSs de reenvío, que lo que harán será reenviar estas peticiones a DNSs de Internet.

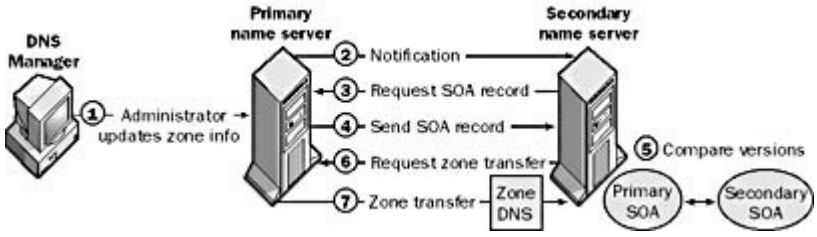
En función de los requisitos, se usarán los mismos o distintos servidores para cada uno de estos DNSs. Generalmente, los DNSs que llevan el espacio de nombres externo estarán en la DMZ, ya que están expuestos al exterior, mientras que los DNSs que llevan el espacio de nombres interno podrán estar en la red interna.

2.4.2 Tipos de DNS

Dentro de la jerarquía de DNS, se establecen zonas del espacio de nombres para la cual hay DNSs **autoritativos**, que son los que tienen el fichero de zona (la base de datos de nombres). Cuando se adquiere un dominio es necesario asociarlo a dos direcciones IP de servidores de nombres autoritativos.

Hay dos tipos de servidores de nombres autoritativos:

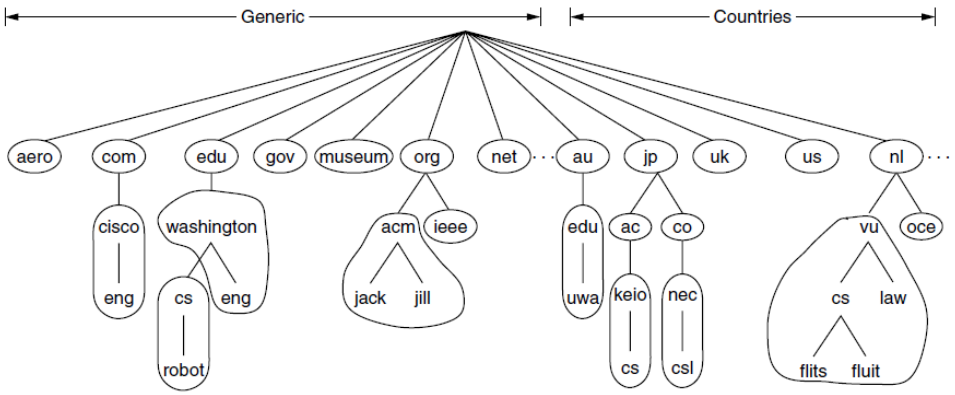
- **Primarios**: Son los que contienen los ficheros de zona con la base de datos de nombre, y pueden ser actualizados.
- **Secundarios**: Contienen una copia de solo-lectura de los ficheros de zona. Esta copia la obtienen de los servidores primarios por un proceso llamado *transferencia de zona* (*zone transfer*). La transferencia de zona puede ser de toda la base de datos de la zona, o incremental, y puede consumir bastante ancho de banda en función del tamaño de la base de datos de nombres. Esto conviene tenerlo en cuenta a la hora del diseño.



Fuente: https://networkencyclopedia.com/zone-transfer/

- Además de estos servidores, también se pueden instalar servidores **locales de reenvío y de solo-caché**, que no son autoritativos y no tienen el fichero de nombres de la zona, sólo se encargan de reenviar consultas a un conjunto de servidores predefinido, y/o realizar consultas y cachearlas.

La división de dominios en zonas depende de los intereses del propietario del dominio. Así por ejemplo, una empresa muy grande puede dividir e dominio en distintas zonas, cada una con sus servidores autoritativos y su fichero de zona. La siguiente figura ilustra esto.



Fuente: Tanenbaum A. S., Wetherall D. J (1981), Computer networks. Pearson. ISBN: 978-0-13-212695-3

2.4.3 Tipos de registros DNS

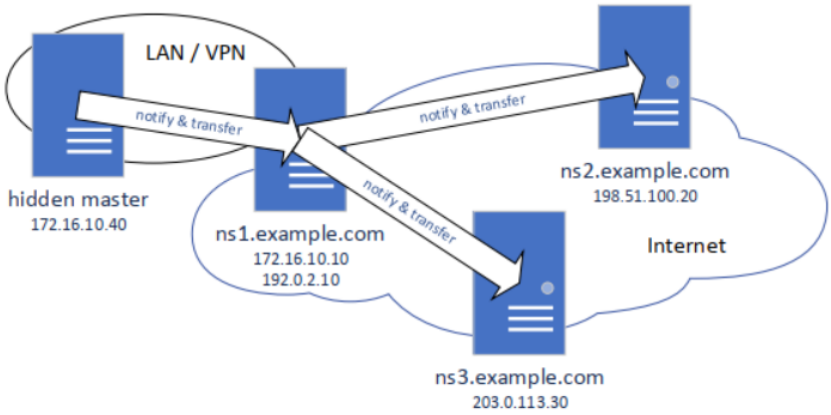
Los registros que se guardan en un servidor DNS pueden ser de distinto tipo en función de la información que almacenan. El listado completo puede verse por ejemplo en la correspondiente página de la wikipedia. En esta práctica usaremos sólo registros de **tipo A**, también llamados de host, que guardan una dirección IP asociada a un nombre de host, y los de **tipo NS**, que indica cuál es el servidor autoritativo de un dominio.

2.4.4 Redundancia

Los DNS suelen ser sistemas críticos y conviene que estén redundados. Se puede conseguir redundancia mediante la instalación de varios DNS secundarios, y servidores de reenvío y/o de solo-caché. Además, se puede conseguir redundancia usando configuraciones de servidores en alta-disponibilidad, que son soluciones ofrecidas por proveedores en las que hay un conjunto de servidores (normalmente dos) completamente replicados y sincronizados, y que funcionan como uno solo, teniendo resiliencia ante el fallo de uno de ellos.

Ya que el servidor autoritativo primario se configura en el registro SOA de DNS, existe también la opción de usar un servidor primario oculto, que no aparece en el fichero SOA de zona, y que se encarga de transferir la zona a otro DNS también primario, el cual sí que aparece en el fichero de zona. Esta sería una configuración más segura, ya que la base de datos real no estaría expuesta al exterior.

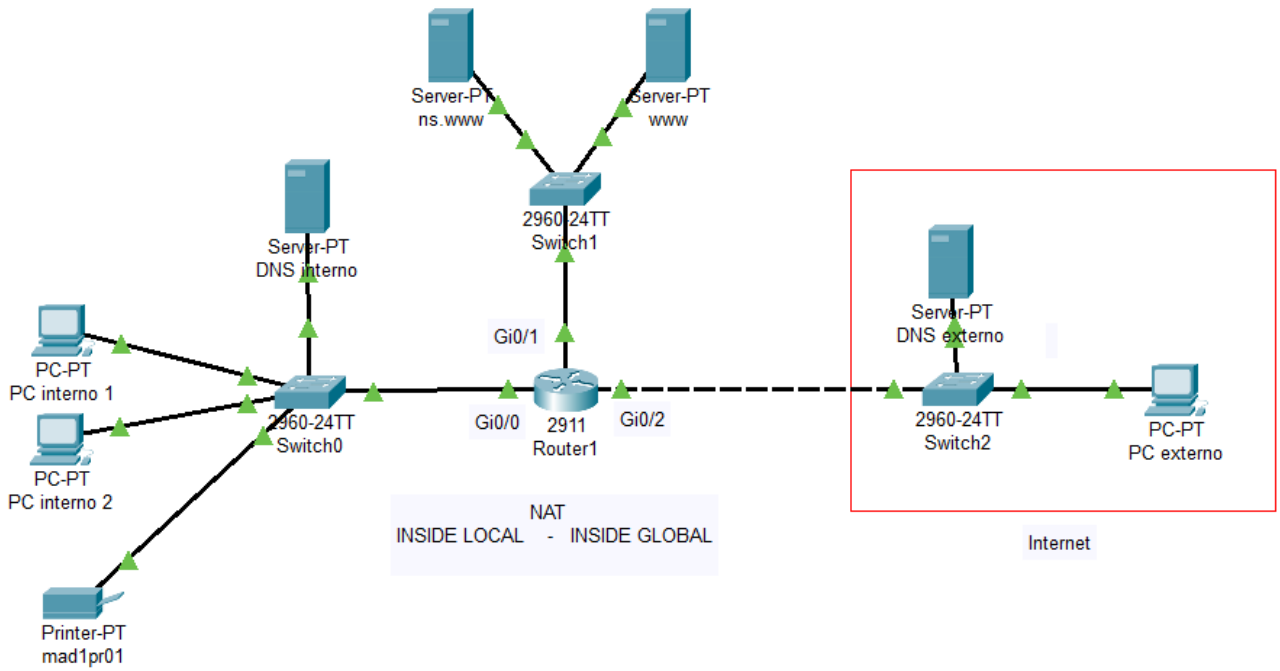
```
$ORIGIN example.com.
@       IN      SOA     ns1.example.com. hostmaster.example.com. (
                        2020053100 ; serial
                        7200       ; refresh (2 hours)
                        3600       ; retry (1 hour)
                        604800     ; expire (1 week)
                        86400      ; minimum (1 day)
                        )
@       IN      NS      ns1.example.com.
@       IN      NS      ns2.example.com.
@       IN      NS      ns3.example.com.

ns1     IN      A       192.0.2.10
ns2     IN      A       198.51.100.20
ns3     IN      A       203.0.113.30
```



Fuente: https://serverfault.com/questions/1019391/what-happens-if-i-do-not-set-my-real-primary-dns-as-soa-entry-in-a-hidden-primar

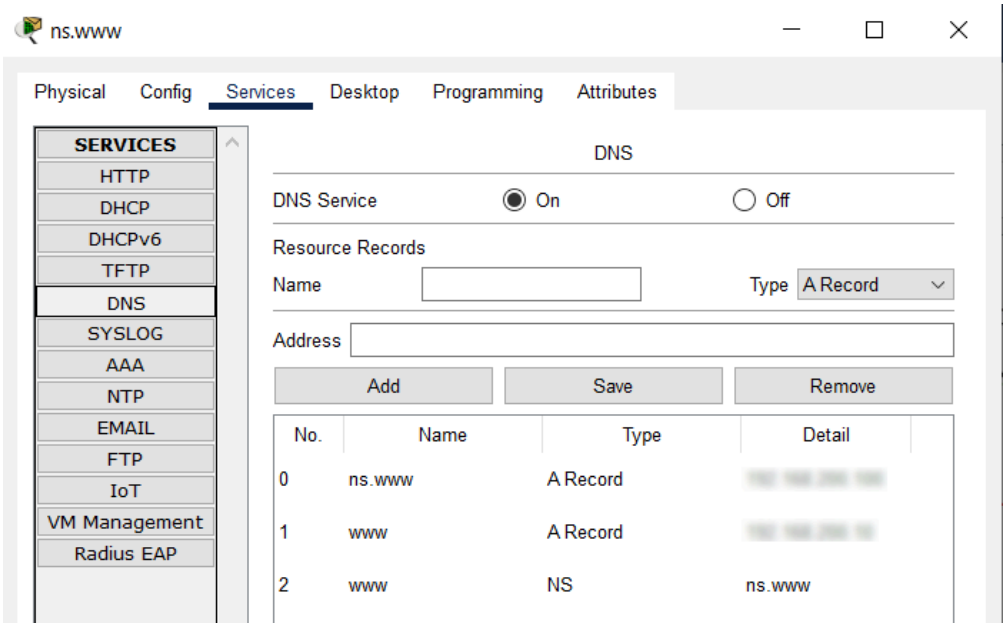
2.4.5 Ejemplo de configuración sencilla de DNS en Packet Tracer

En esta práctica vamos a realizar una configuración sencilla de DNS en Packet Tracer, dentro de las posibilidades que tiene este programa, que no son muchas, ya que no permite configurar servidores primarios y secundarios. Trabajaremos con la red de la siguiente figura.



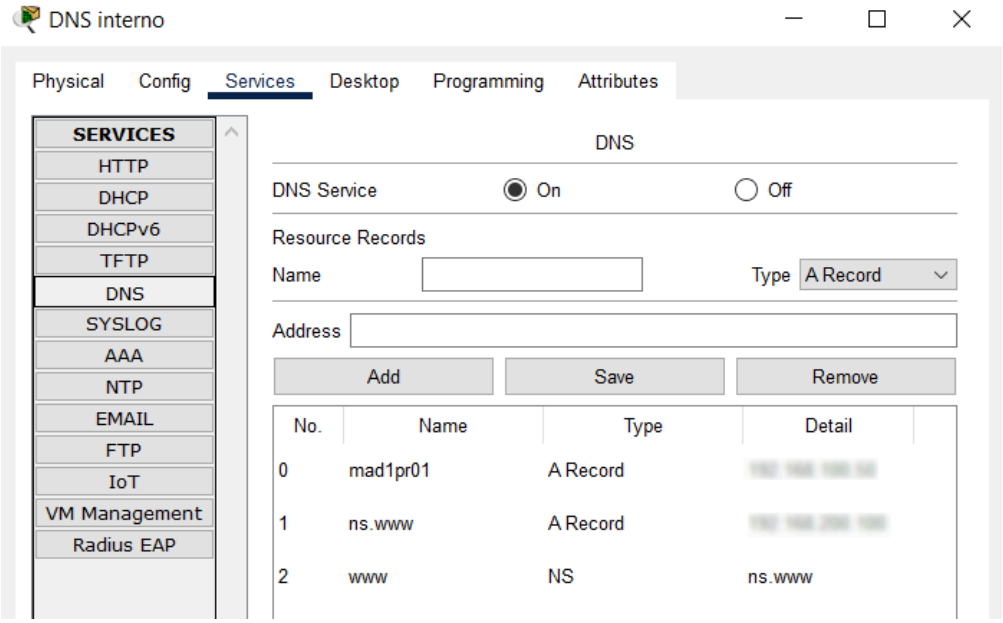
En este ejercicio vamos a ilustrar la división de una red en un dominio de nombres interno y otro externo, y también la noción de servidor autoritativo, para lo cual requeriremos registros DNS de tipos A y NS.

- En primer lugar configuraremos el servidor DNS ubicado en la DMZ, ns.www, que sería el servidor autoritativo del dominio www. Este servidor almacenará la información del servidor autoritativo del dominio (él mismo), así como la información de los hosts en el dominio, en este caso únicamente el servidor web www, cuyo nombre corresponde con el del dominio (aunque también lo podríamos haber llamado, por ejemplo, web.www). La siguiente figura muestra dicha configuración.

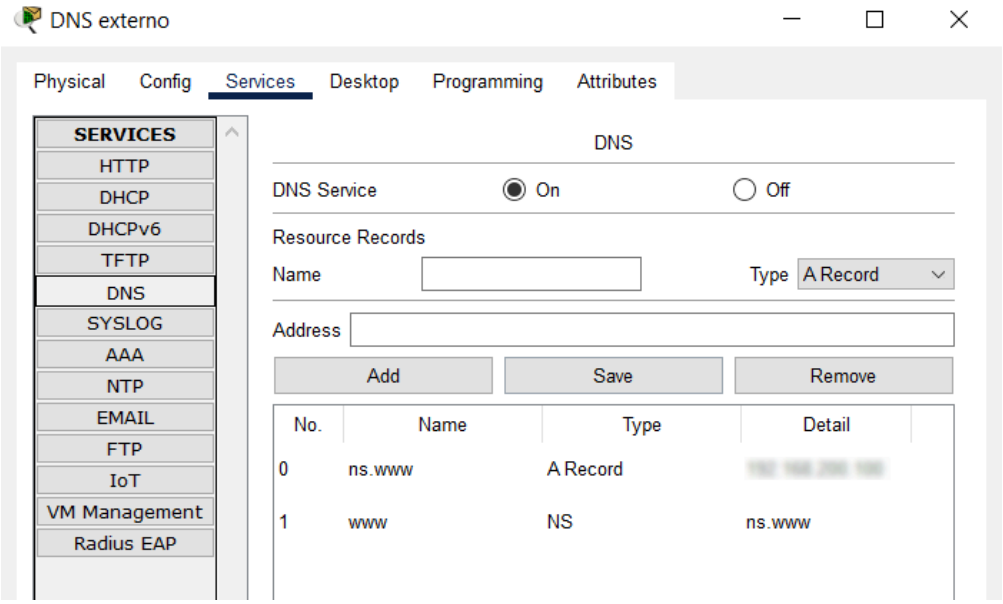


- En segundo lugar configuraremos el servidor DNS interno. Este servidor guardará los

registros de nombres internos de la corporación, que no deben conocerse en el exterior, como por ejemplo el de la impresora mad1pr01. El servidor también almacenará la información del servidor de nombres autoritativo del dominio www (es decir, ns.www), de forma que las consultas correspondientes a nombres de este dominio se enviarán a dicho servidor. En la siguiente figura puede verse la configuración necesaria.



- Por último configuraremos el servidor DNS externo, ubicado en internet, el cual almacena la información del servidor autoritativo del dominio www.



Con ello quedarían configurados los DNS. Podemos comprobar el funcionamiento activando el modo simulación, con los filtros de los protocolos DNS, HTTP e ICMP, y probando a acceder a

la web www desde un host interno y otro externo, y haciendo ping desde un host interno al nombre mad1pr01.

2.5 Network Address Translation (NAT)

NAT es la traducción de las direcciones IP origen o destino de la cabecera IP por otras. Un dispositivo que realiza NAT (también llamado gateway NAT) guarda una tabla de traducciones, y así, cuando le llega un paquete IP, comprueba las direcciones IP origen y destino y la tabla de traducciones, y reemplaza la dirección IP que corresponda en la cabecera IP (ninguna, origen, destino o ambas). NAT permite que hosts a un lado del dispositivo NAT aparezcan al otro lado con otras direcciones IP distintas a las que tienen realmente. Esto es muy útil, por ejemplo, para el acceso a internet, ya que una red puede usar internamente direccionamiento privado, y hacer NAT para el tráfico con internet. Esto permite utilizar únicamente el direccionamiento IP imprescindible, y ahorrar direcciones IP. Sin el direccionamiento privado y NAT, hace muchos años que las direcciones IPv4 se habrían agotado. Por otro lado, NAT tiene la desventaja de que hay aplicaciones y protocolos que incluyen la dirección IP no sólo en la capa IP, sino en las cabeceras de otras capas, o incluso en el campo de datos. En esos casos, o bien el dispositivo NAT es capaz de reescribir las direcciones IP en todos esos campos al hacer la traducción (lo que se denomina NAT transversal), o bien la aplicación o servicio correspondiente no funcionará, y no se podría hacer NAT.

NAT es imprescindible cuando se usa direccionamiento privado en la red interna y existe comunicación entre la red interna y usuarios o servicios en Internet, ya que el direccionamiento privado no puede salir a Internet. También es imprescindible cuando se interconecta una red con direccionamiento privado con otra externa que también usa direccionamiento privado. En estos casos, habrá que traducir estas direcciones por otras públicas.

Hay distintos tipos de NAT:

- **NAT estático**: Existe un mapeo de direcciones IP una a una. A una dirección IP le corresponde otra específica.
- **NAT dinámico**: El mapeo de dirección IP por otra se realiza dinámicamente, entre un pool de direcciones IP disponibles para la traducción. Normalmente habrá pocas direcciones IP traducidas (por ejemplo, pocas direcciones IP públicas), ya que en el momento en que un flujo ha terminado, la dirección IP traducida queda libre para el siguiente flujo. Sin embargo, si la demanda de traducciones es elevada en un determinado momento, y ya no quedan IPs libres en el pool, los paquetes que no pueden traducirse se descartarían.
- **NAT con sobrecarga** (NAT overload): Es un tipo especial de NAT dinámico, en el que si no quedan IPs en el pool de IPs traducidas, entonces se traducen también puertos. Un caso especial de NAT con sobrecarga es cuando se usa un pool de una única dirección IP (por ejemplo, una única dirección IP pública), y todas las direcciones IP de la red interna se traducen por ésta. Para poder distinguir el tráfico de cada host interno, se traduce también el puerto, y el gateway NAT guarda una tabla de direcciones IPs y puertos. Este caso se denomina **PAT (port address translation)**, y es el que típicamente utilizan los routers de acceso a internet que se tienen en casa.

2.5.1 NAT y redundancia

Cuando hay varios routers que interconectan con el ISP existe un problema con el NAT si estos routers no tienen la base de datos de NAT sincronizada y no se usa routing dinámico (típicamente BGP) entre la organización y el ISP. El problema ocurriría ya sea cuando los paquetes de una comunicación entre un host interno que usa NAT y uno externo salen hacia fuera de la red por distinto router, o bien cuando los paquetes de ida no usan el mismo router que los de vuelta. En cualquier circunstancia, si algunos paquetes de cualquiera de las dos direcciones del tráfico van por distinto router, la comunicación no funcionará. En este caso, la solución es usar un protocolo de enrutamiento dinámico entre la organización y el ISP para forzar a que los paquetes vayan siempre por el mismo gateway NAT (lo cual es complejo), o bien emplear routers que soporten algún tipo de sincronización de la base de datos de NAT. Hay distintas soluciones en el mercado (algunas trabajan en activo/activo, otras en primario/secundario). Para el proyecto de la asignatura, si se usa redundancia en la conexión al ISP y NAT, habría que considerar este caso y contemplar equipos que lo soporten, pero para la implementación de packet tracer sería suficiente con usar dos routers con NAT, y suponer que la base de datos de NAT está sincronizada.

2.5.2 Direccionamiento privado o público en DMZ

Ya sabemos que los servicios de la red que estén accesibles desde el exterior tendrán que tener direccionamiento público para que tengan alcanzabilidad desde el exterior. Sin embargo, existen las opciones de que este direccionamiento público se consiga mediante NAT, o bien los servidores usen direcciones IP públicas. Cada opción tiene sus ventajas y sus inconvenientes

- Direccionamiento privado en DMZ + NAT. Esto facilita que los usuarios dentro de la red interna puedan acceder a los servicios de la DMZ usando direccionamiento privado. Por ejemplo, sería sencillo que accediesen a un servidor Web. Por el contrario, los usuarios externos accederían a una dirección IP pública estática configurada en el gateway NAT. El principal inconveniente que puede tener esta opción es que algún servicio de la DMZ no soporte NAT.
- Direccionamiento público en DMZ. Esto permite que todos los servicios de la DMZ funcionen bien, ya que no tendrán un NAT entre ellos y los usuarios externos. Sin embargo, dificulta el acceso a los servicios de la DMZ por parte de los usuarios internos si éstos usan direccionamiento privado. En este caso, las opciones serían:
    - Crear enrutamiento dentro de la red interna para la subred pública de la DMZ. Esta puede ser una solución compleja.
    - Configurar NAT hairpinning. Esto consiste en configurar en el router NAT que las peticiones desde la red interna a las direcciones IP públicas de los servicios de la DMZ vayan a la DMZ. Es una configuración algo compleja que queda fuera del alcance de la asignatura.
    - Asignar doble direccionamiento IP a los servicios de la DMZ, privado y público, y configurar los servicios con direccionamiento privado en el DNS de espacio de nombres interno. Esta solución implica que el mantenimiento del fichero de zona de los DNSs se complica.

2.5.3 Orden de procesamiento en routers Cisco de ACL y NAT

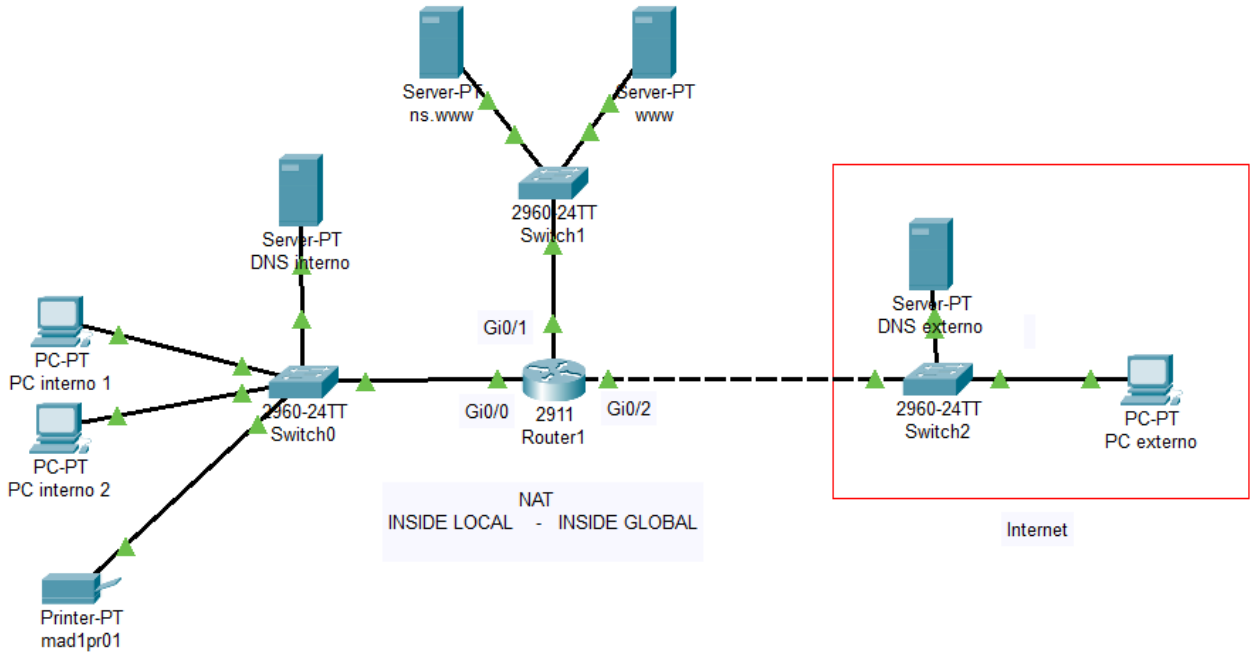
Hay que tener cuidado cuando se configura en los routers varias funcionalidades que hacen uso de las direcciones IP. Por ejemplo, si se configura un ACL y NAT, es importante saber qué direccionamiento habrá que poner en el ACL. Para esto es necesario conocer el orden en que un router procesa ACLs y NAT.

Los siguientes recursos explican el orden que sigue un router Cisco:

- Cisco NAT order of operation
- Order of operation NAT + routing + ACL

2.5.4 Configuración de NAT en una red sencilla

En el laboratorio vamos a configurar NAT en el router de la misma red con la que hemos estado trabajando, como ejemplo de configuración de NAT en un router Cisco.



Cisco utiliza las palabras clave **inside** y **outside** para indicar las interfaces interna y externa en NAT. Además, utiliza las palabras clave **local** y **global** para indicar si el direccionamiento es el que se ve en la red interna, o el que se ve en la red externa. Así tenemos direcciones de los siguientes tipos:

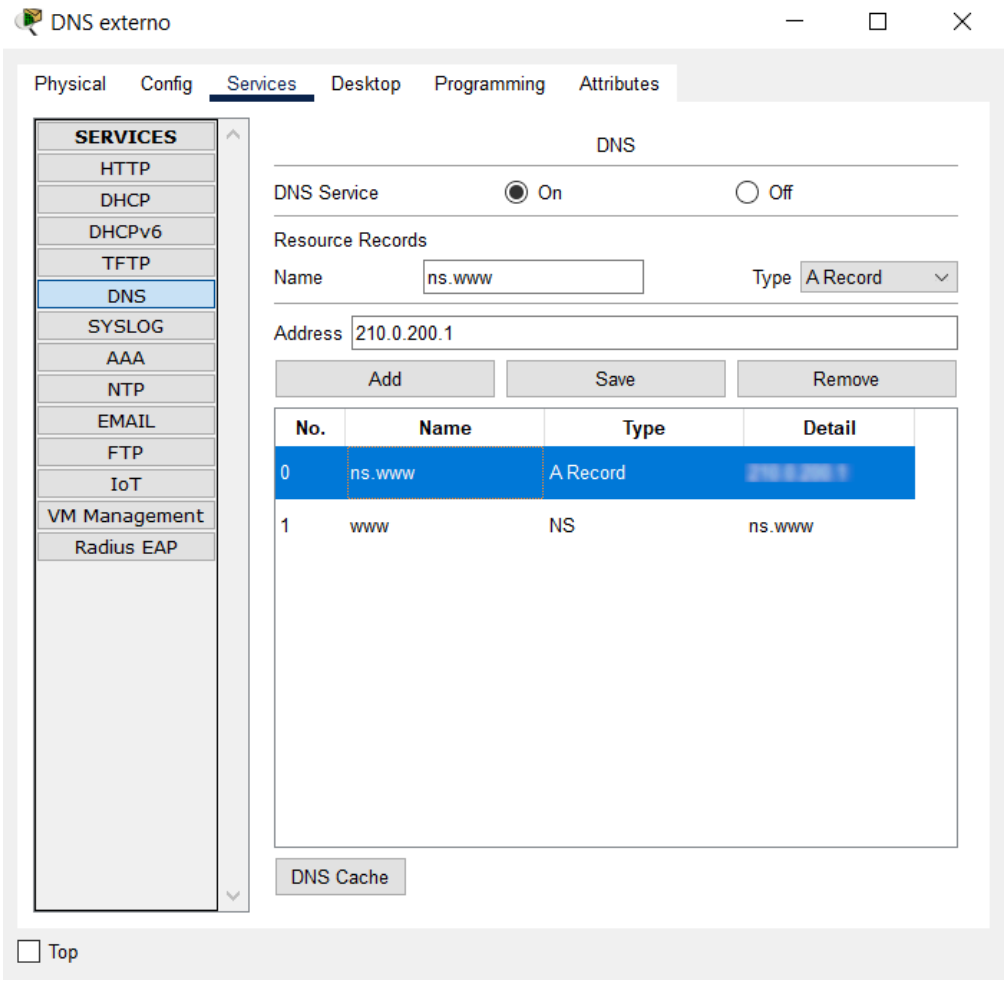
- **Inside local**: Direcciones asignadas a dispositivos internos. Estas direcciones no son anunciadas al exterior.
- **Inside global**: Direcciones por las que los dispositivos internos son conocidos en el exterior.
- **Outside local**: Direcciones por los que los dispositivos externos son conocidos en la red interna.

- **Outside global**: Direcciones asignadas realmente a los dispositivos externos. Estas direcciones no son anunciadas en la red interna.

En nuestra red, lo que queremos es asignar direcciones públicas estáticas a los servidores DNS y Web, que son accesibles desde el exterior, y una dirección pública (por lo tanto PAT), para todos los hosts de la red interna. En este caso traduciremos direcciones *inside local* por inside *global*, y no necesitaremos traducir las direcciones IP de los dispositivos externos. Para ello seguiremos los pasos que se indican a continuación.

1. Cambio de IP de servidor DNS ns.www en el servidor DNS externo

Una vez configuremos NAT deberíamos poder acceder a los servidores DNS y Web de la red interna desde internet usando sus direcciones IP públicas. Sin embargo, en el servidor DNS externo, ns.www está asociado a la dirección IP privada. Vamos a cambiarla en el DNS externo por la dirección IP pública que configuraremos después, tal y como indica la siguiente figura. Después de hacerlo, es conveniente **borrar la caché del servicio DNS**.



2. Configuración de NAT estático para los servidores

A los servidores les asociaremos siempre las mismas direcciones IP públicas, ya que deben poder ser accedidos desde el exterior. Para ello es necesario usar NAT estático. NAT estático se configura primero asociando una dirección IP interna con su traducida en el exterior, y a continuación configurando las palabras clave inside y outside a las interfaces interna y externa en las que el router debe realizar el NAT.

```
Router#conf t
Router(config)#ip nat inside source static
[ip_a_traducir_servidor_Web] [ip_traducida_servidor_Web]
Router(config)#ip nat inside source static
[ip_a_traducir_servidor_DNS] [ ip_traducida_servidor_DNS]
Router(config)#int [interfaz_interna]
Router(config-if)#ip nat inside
Router(config-if)#int [interfaz_externa]
Router(config-if)#ip nat outside
```

Una vez configurado esto, se puede comprobar el funcionamiento intentando acceder desde navegador web del PC externo a la web www. En modo simulación debería verse cómo el router traduce la dirección IP de los servidores internos. También en DNS externo guardará en caché la IP pública del servidor Web. En el router se puede observar la tabla de traducciones con el siguiente comando.

```
Router#show ip nat translations
```

3. Configuración de PAT para la red interna

En la red interna configuraremos una única dirección IP para todos los dispositivos, de forma que se haga PAT para poder usar simultáneamente la misma IP pública en todos ellos, cambiando el puerto. La configuración de PAT es un poco más compleja que la de NAT estático:

- Hay que configurar el rango de direccionamiento interno a traducir mediante una ACL. (*Éste es un ejemplo de uso de ACLs en donde no se usan para descartar tráfico*).
- Hay que configurar el pool de direcciones IP externas (en este caso, sólo una) y darle un nombre.
- Hay que configurar la traducción del rango anterior por el pool anterior, indicando que además se realiza overload.
- Igual que en el NAT estático, hay que configurar las interfaces involucradas como inside

u outside.

```
Router(config)#access-list [ID_ACL] permit [subred_interna]
[wildcard_mask]
Router(config)#ip nat pool [nombre_pool] [IP_traducida]
[IP_traducida] netmask [máscara]
Router(config)#ip nat inside source list [ID_ACL] pool [nombre_pool]
overload
Router(config)#int [interfaz_interna]
Router(config-if)#ip nat inside
```

Una vez configurado esto, se puede comprobar el funcionamiento realizando ping, en modo simulación, entre algún PC interno y el PC externo. Al igual que antes, en el router se puede ver la tabla de traducciones con el siguiente comando.

```
Router#show ip nat translations
```

3. Multilayer switching

3.1 Objetivo

El objetivo de esta práctica es comprender la ventaja del uso de multilayer switches, y familiarizarse con la configuración de este tipo de dispositivos en Cisco, que tiene alguna particularidad con respecto a la configuración de switches y routers.

3.2 Competencias

Tras la finalización de la práctica deberían haberse adquirido las siguientes competencias:

- Conocer qué es y para qué sirve un multilayer switch.
- Conocer las ventajas de usar multilayer switches en la capa de distribución de una red jerárquica.
- Saber cómo configurar en multilayer switches spanning tree, HSRP, interfaces VLAN, interfaces IP y RIP.

3.3 Enlaces de interés

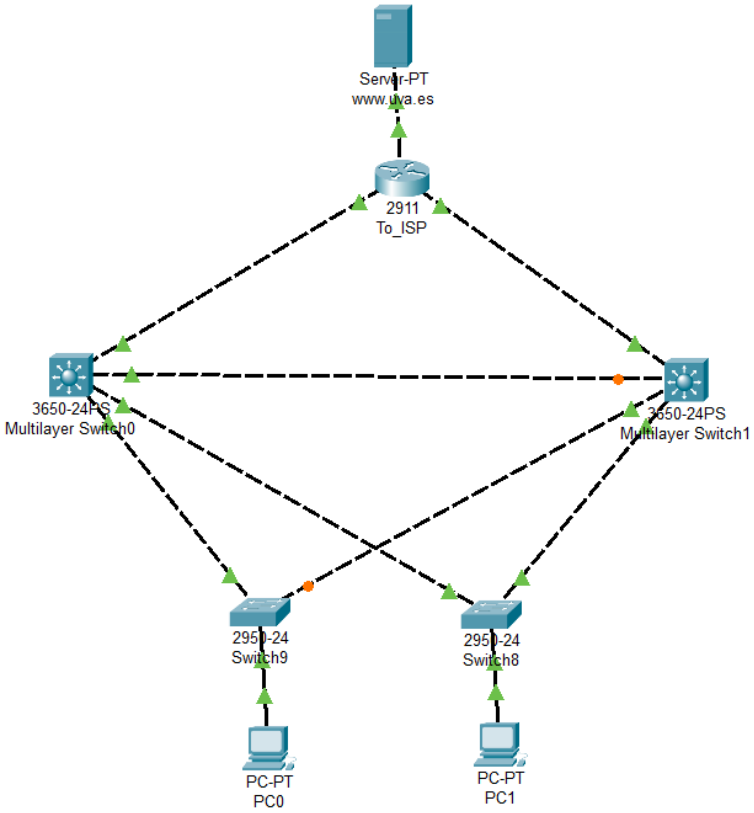
A continuación se indican algunos recursos que explican cómo configurar un multilayer switch en packet tracer.

- InterVLAN routing en switches de capa 3:
  - Implementing Inter-VLAN Routing
  - Configure InterVLAN Routing on Layer 3 Switches
  - Cisco Layer 3 Switch InterVLAN Routing Configuration (recurso de la carpeta CCNA de la asignatura)
- HSRP en interfaz svi
  - HSRP (Hot Standby Routing Protocol)

3.4 Configuración de red jerárquica con multilayer switches

Hay algunos dispositivos que actúan como switches y routers. Estos dispositivos suelen llamarse multilayer switches (conmutadores multicapa), o layer 3 switches (conmutadores de capa 3). La configuración de estos equipos puede tener alguna particularidad con respecto a la configuración que hemos visto hasta ahora en la asignatura de switches y routers. Para aprender a configurar estos dispositivos y comprender sus ventajas, vamos a usarlos en la red con la que trabajamos en la práctica 2. La red redundante creada en el ejercicio 2 de laboratorio puede optimizarse, reemplazando dos switches y dos routers por dos multilayer switches. Puede verse en la imagen siguiente la topología de la red resultante. En esta práctica

partimos de una red con alguna configuración hecha, como las direcciones IP de los hosts, del servidor, y de las interfaces IP del router, pero el resto de configuración falta, y es la que vamos a realizar en este laboratorio. Para ello seguiremos los pasos que se indican a continuación.



1. **Configurar puertos modo access/trunk en todos los switches** (como en cualquier switch).

2. **Configurar VTP y VLANes en los switches** (como en cualquier switch).

3. **Configurar PVST en los switches** (como en cualquier switch).

4. **Activar IP routing en los multilayer switches para que funcione el routing IP** (la capa 3).

   Esto hay que hacerlo antes de meter comandos de configuración de IP.

   ```
   (config)# ip routing
   ```

5. **Configurar dirección IP y HSRP en multilayer switches en interfaces hacia switches de**

acceso.

En un multilayer switch la config de IP de VLANes no va en subinterfaces, como en los routers, sino en interfaces virtuales llamadas "svi" (switched virtual interfaces). Estas interfaces corresponden con la VLAN: interface vlan 30.

```
(config)# interface vlan [VLAN_ID]
(config-if)# [aquí toda la config ip, como la dirección ip y
hsrp]
```

Al crear la svi (la interfaz vlan) debería crearse automáticamente la VLAN en el switch. Si no es asi, hay que crearla manualmente como en cualquier switch. Si no está creada, no levantará la interfaz VLAN. En nuestro caso, ya la deberíamos haber creado en el paso 2.

6. **Configurar en los multilayer switches las interfaces IP conectadas con el router.**

   En las interfaces IP en las que no van a ir VLANes (por ejemplo, en este caso, en la interfaz contra el router), hay que desactivar el switching en la interfaz para poder configurar la IP. Luego ya se puede configurar la IP como en un router normal.

```
(config)# interface [puerto]
(config-if)# no switchport
(config-if)# ip address [dirección_IP] [máscara]
```

7. **Configurar el routing dinámico** (rip, ospf, etc).

   En este caso, configurar RIP en los multilayer switches y en el router.

8. **Si aplica, sumarizar anuncios de rutas hacia el core** (si lo permite el switch y packet tracer).

   En este caso, como estamos usando RIPv1, no es necesario, ya que RIPv1 sumariza a la clase por defecto (esto se ve en la teoría y en las prácticas de routing).

4. Control de acceso a puerto de switch

4.1 Objetivo

El objetivo de esta práctica es conocer dos formas de proteger el acceso cableado a un switch: filtro de direcciones MAC y 802.1x.

4.2 Competencias

Tras la finalización de la práctica deberían haberse adquirido las siguientes competencias:

- Conocer la funcionalidad port security de Cisco y cómo configurarla.
- Conocer qué es, para qué sirve, y cómo funciona, el estándar IEEE 802.1x en una red cableada.
- Saber cómo configurar 802.1x en una red con switches y routers Cisco.

4.3 Enlaces de interés

- Implementar port-security
- Introducción a la Autenticación 802.1x
- Catalyst 2960-X Switch Security Configuration Guide, Cisco IOS Release 15.0(2)EX
- Control de acceso a red basada en puertos IEEE 802.1X (youtube)

4.4 Control de acceso a puerto de switch

Los dispositivos de capa 2, como los switches, son un punto débil para accesos no autorizados si no están protegidos, ya que en muchas ocasiones sólo sería necesario conectar un portátil a un puerto libre ethernet para ganar acceso a la red. Aunque esto requiere acceso físico a dicho puerto, muchas veces es algo sencillo de conseguir en muchas corporaciones, y en muchos casos, si está activo DHCP, un usuario malicioso estaría automáticamente conectado a la red con sólo conectar su portátil a un puerto de red libre.
Hay distintas formas de proteger el acceso a la red en la capa 2. En este laboratorio veremos las dos siguientes:

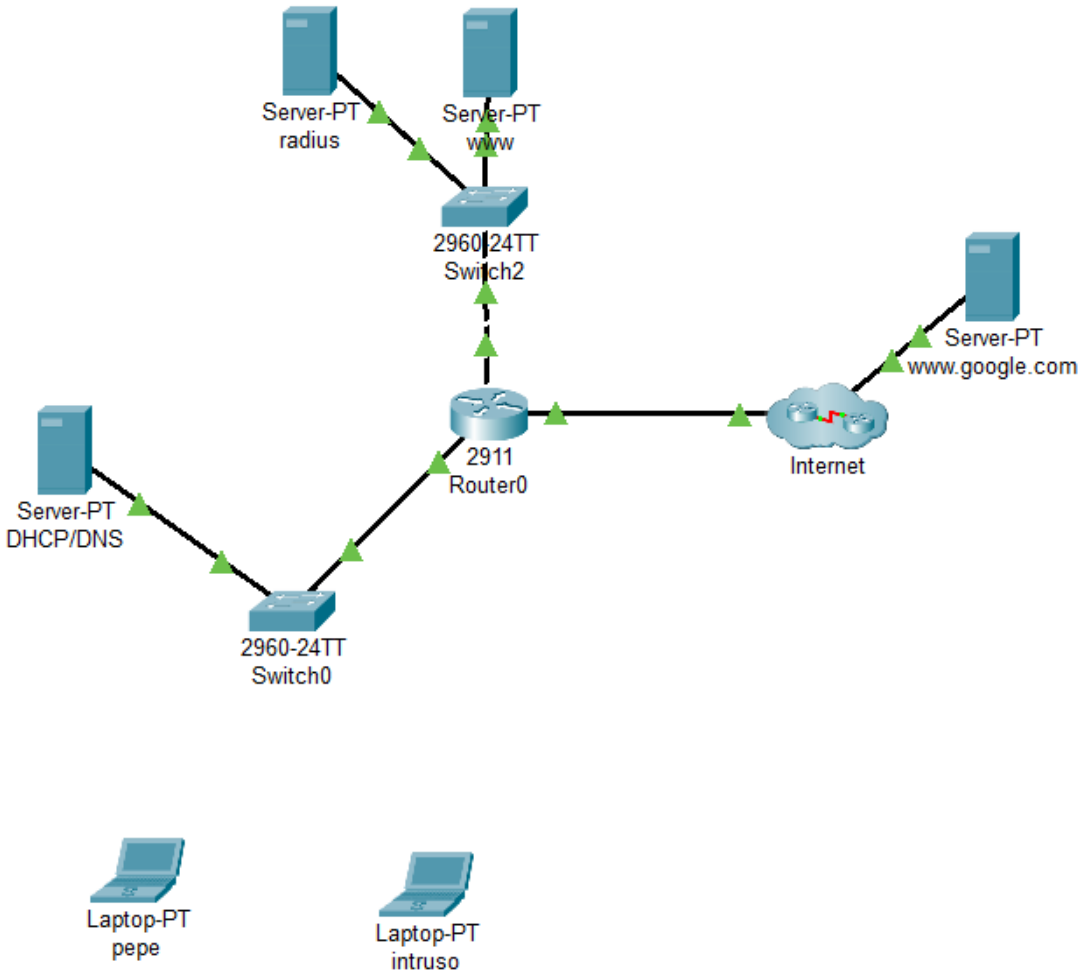
- Activando un filtro de direcciones MAC en el propio switch. La mayoría de proveedores de switches profesionales implementan funcionalidades para configurar las direcciones MAC permitidas en los puertos del switch. En Cisco esta funcionalidad se llama "Cisco Port Security".
- Utilizando el estándar 802.1X, control de acceso a red basada en puertos, que permite la autenticación, por ejemplo, vía usuario y contraseña o certificado, de dispositivos conectados a un puerto.

Otra forma de control, que no sería en la capa 2, pero que utiliza un filtro de MAC, sería usando direccionamiento IP manual por DHCP, asignando una IP estática a cada dirección MAC. Esto se configuraría en el servidor DHCP, si éste lo permite. Requiere cierto trabajo de mantenimiento para las altas y bajas de las asignaciones. Tiene la desventaja de que si bien impediría la conexión a nivel IP de un usuario no autorizado, éste tendría acceso a nivel 2 al switch, y podría efectuar algún ataque.

Por último, es muy recomendable que los puertos que no se vayan a usar de un switch estén desactivados por configuración (en cisco mediante el comando shutdown a nivel de interfaz).

4.5 Configuración de control de acceso a puerto de switch

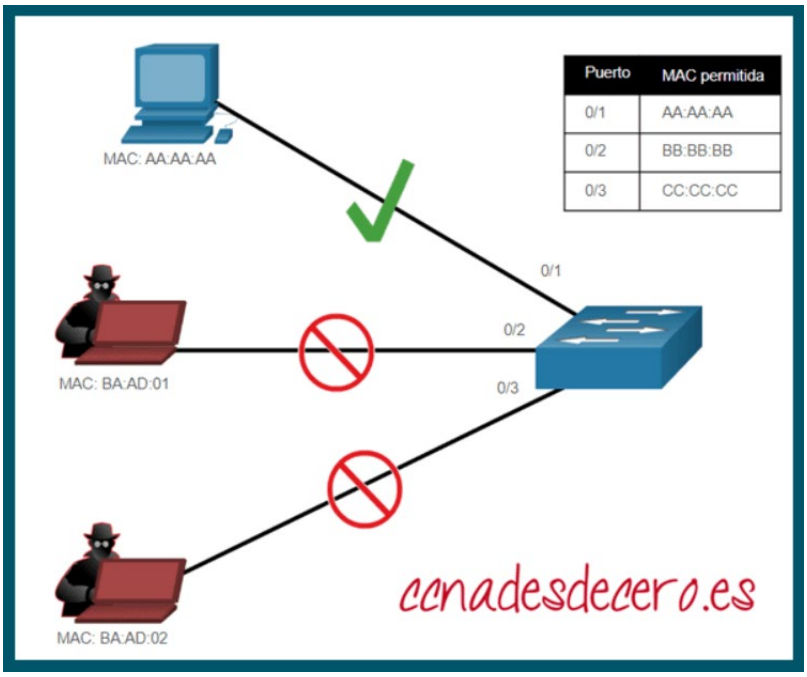
En esta práctica vamos a configurar port security y autenticación vía 802.1X en una red sencilla usando Packet Tracer, y observaremos su funcionamiento. Vamos a trabajar con la red de la siguiente imagen. Toda la configuración de direccionamiento IP y routing está preconfigurada, excepto aquella necesaria para configurar port security y 802.1X. También está configurado un servidor DHCP y DNS, y varios servidores Web.



4.5.1 Configuración de Cisco Port Security

Cisco Port Security es la funcionalidad de switches Cisco que permite especificar las direcciones MAC autorizadas para conectarse a un puerto del switch. La funcionalidad tiene algunos parámetros de configuración que permiten, o bien indicar manualmente las MACs autorizadas o bien aprenderlas dinámicamente, definir un número máximo de MACs autorizadas, especificar el tiempo durante el cual dichas MACs están permitidas, y definir la acción en caso de intento de acceso de una MAC no permitida.

Esta funcionalidad previene que un atacante se conecte al switch (aunque siempre podría cambiar la dirección MAC de su terminal), y también previene ataques de desbordamiento de la tabla MAC. Estos ataques consisten en generar mucho tráfico usando múltiples direcciones MAC origen, de forma que se llene (se inunde) con ellas la tabla de MAC del switch. Cuando esto ocurre, el switch reenviará por todos sus puertos todos los paquetes de tráfico real, y el atacante podrá verlos.



Fuente: https://ccnadesdecero.es/implementar-port-security/

En este laboratorio vamos a realizar una configuración sencilla en la que autorizaremos la MAC del portátil del empleado pepe en la interfaz fa0/4 del Switch0. Para ello seguiremos los pasos que se indican a continuación.

1. **Configuración de port security en el switch**

```
Switch#conf t
Switch(config)#int fa0/4
Switch(config-if)#switchport mode access          #necesario
para port-security que el modo no sea dinámico
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address
[dirección_MAC_pepe]
Switch(config-if)#switchport port-security maximum 1     #por
defecto es 1, pero lo ponemos para ver el comando
```

2. **Verificación de port security**

Podemos comprobar la configuración de port security con los siguientes comandos:

```
Switch# show port-security
Switch#show port-security int fa0/4
Switch#show port-security address
```

A continuación, comprobamos que si conectamos el portátil de pepe en la interfaz fa0/4, se establece conexión, y podemos por ejemplo hacer ping a cualquier servidor. Desconectamos el portátil de pepe y conectamos el portátil del intruso en la interfaz fa0/4. La interfaz no levantará. En packet tracer se indica con el cable en rojo (puede tardar unos segundos). En ese caso la interfaz pasa a estar en estado "error-disabled", y sólo levantará si desactivamos y activamos el puerto. (*Este comportamiento es configurable mediante la opción "violation" del comando switchport port-security*).
Para ver el estado del puerto cuando el cable está en rojo:

```
Switch#show interfaces status
```

Desconectamos el cable, y a continuación reiniciamos el puerto y comprobamos de nuevo el estado:

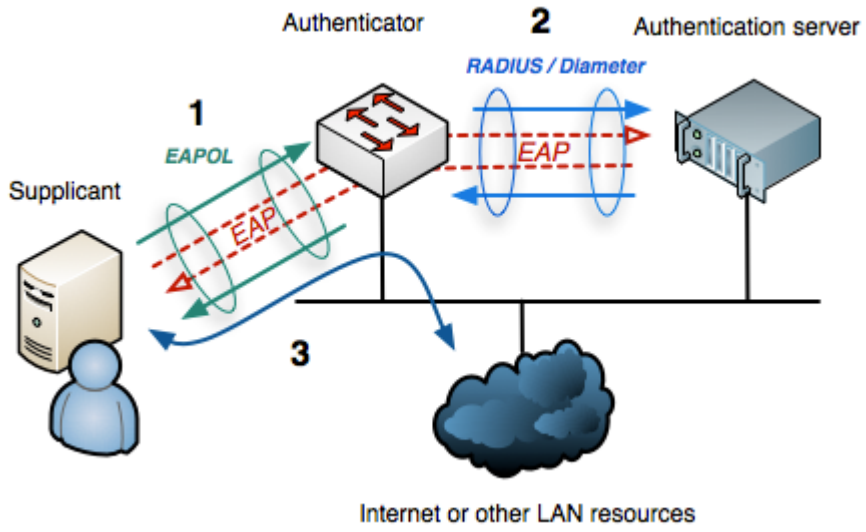
```
Switch#conf t
Switch(config)#int fa0/4
Switch(config-if)#shutdown
Switch(config-if)#no shutdown
Switch(config-if)#^Z
Switch#show interfaces status
```

4.5.2 Configuración de 802.1X

802.1X es un estándar de la IEEE que permite el control de acceso a una red basado en puertos, de forma que un dispostivo que se conecta a un puerto de la red, debe autenticarse para poder acceder a la misma. 802.1X se usa tanto en redes inalámbricas como en redes cableadas. En el estándar 802.1X hay tres componentes: cliente (o suplicante), dispositivo de acceso (o autenticador), y servidor de autenticación.

Fuente: https://forum.huawei.com/enterprise/es/introducci%C3%B3n-a-la-autenticaci%C3%B3n-802-1x/thread/513787-100239

El cliente es el dispositivo que intenta acceder a la red. El dispositivo de acceso es el elemento al que se conecta el cliente, y que impide su acceso mientras no se autentique. Actúa como pasarela de autenticación entre el cliente y el servidor de autenticación, que es el componente que proporciona el servicio de autenticación, y lleva a cabo la autenticación, autorización y contabilidad (AAA). El servidor de autenticación suele ser un servidor Radius. 802.1X usa EAP como protocolo de autenticación entre cliente y servidor de autenticación. En el caso de redes cableadas, normalmente EAP va en capsulado en EAPoL entre cliente y dispositivo de acceso y en Radius entre el dispositivo de acceso y servidor Radius. En esta práctica vamos a centrarnos en una red cableada.



Fuente: By Arran Cudbard-Bell Arr2036 [GFDL (http://www.gnu.org/copyleft/fdl.html)], via Wikimedia Commons

En una red cableada, 802.1X permite un control de acceso a un puerto, por ejemplo de un switch, de manera que el usuario que se conecta al puerto debe autenticarse, por ejemplo con un certificado o mediante usuario y contraseña. Con esto se consigue una protección más eficiente y ágil que otros sistemas de control de acceso, como aquellos basados en MAC, en donde hay que habilitar explícitamente las direcciones MAC de los dispositivos a los que se permite el acceso. Si nos imaginamos una oficina de una empresa donde los empleados cuando llegan conectan su portátil a una toma de red, 802.1X obligaría al usuario a autenticarse en la red al conectarse, evitando que un intruso pueda conectar su portátil a una toma de red y tener acceso a la misma.

En esta práctica configuraremos el Switch0 2960-24TT como autenticador 802.1X y activaremos 802.1X en las interfaces Fa0/1, Fa0/2 y Fa0/3. La versión mínima de Cisco IOS

(el sistema operativo de Cisco) en un switch para que soporte 802.1X es la 15.0. Puede verse la versión de IOS que corre un equipo Cisco con el comando 'show version'.

Configuración Switch0

1. **Configuración de dirección IP del Switch.** En la red de la figura los empleados se conectan a la VLAN 10. El Switch0 ya tiene configurados los puertos Fa0/1 al Fa0/4 en la VLAN 10, y el resto de puertos no usados están desactivados (shutdown). El protocolo EAPoL va sobre Ethernet, pero el protocolo Radius va sobre IP, por lo que el Switch0 necesitará tener conectividad IP con el servidor Radius. Debido a ello tendremos que configurarle una dirección IP, y un default gateway hacia el router, esto último porque las IPs de Switch0 y Radius no pertenecerán a la misma subred. Configuraremos la dirección IP en la VLAN 1 (VLAN por defecto). El default gateway se configura a nivel global, no a nivel de interfaz VLAN.

```
int vlan1
 ip address [ip_switch] [máscara]
 no shut
 exit
ip default-gateway [ip_router]
```

2. **Configuración de autenticación radius en 802.1X**. Para ello es necesario activar AAA, configurar el servidor Radius, indicando su IP, el puerto que se usará, y la clave compartida, y activar que en 802.1X se autentique vía Radius.

```
aaa new-model
radius-server host [ip_radius] auth-port [puerto] key [psk]
aaa authentication dot1x default group radius
```

3. **Configuración de 802.1X.** Es necesario activar 802.1X a nivel global, y en las interfaces. En las interfaces además hay que indicar que el dispositivo actúa como autenticador. En nuestro caso vamos a configurar el acceso vía 802.1X en las interfaces fa0/1, fa0/2 y fa0/3.

```
dot1x system-auth-control

interface range Fa0/1-Fa0/3
 switchport mode access
 authentication port-control auto
 dot1x pae authenticator
```

Configuración Router0

En el router hay que configurar la dirección IP para la VLAN 1, que es la que usará el Switch para comunicarse con el servidor Radius. Para configurar esta IP, podemos hacerlo en una subinterfaz, pero también podemos configurarla a nivel de interfaz, dado que la VLAN 1 por defecto es la VLAN nativa (que significa que no usa etiquedado de VLAN 802.1q). Lo vamos a hacer de esta última forma.

```
int gi0/0
ip address [ip_router] [máscara]
```

Configuración Servidor Radius

1. En el servidor Radius hay que configurar el servicio AAA (Radius). En la parte de 'Network Configuration' hay que añadir los clientes radius, es decir, los dispositivos desde donde llegarán las peticiones de autenticación Radius. En este caso el cliente será el Switch0. Le daremos un nombre cualquiera (es un mero ID local), por ejemplo switch0, la IP que hemos configurado en el Switch, 192.168.1.2, y una clave compartida o secret, que tendrá que ser la misma que configuramos en el switch (por ejemplo, 123456). En la parte de 'User Setup' hay que configurar los nombres de usuario y contraseñas de los usuarios, por ejemplo, pepe /pepe. Finalmente, activar el servicio (Service -> ON).

2. En el servidor Radius también es necesario configurar el servicio Radius EAP, permitiendo EAP-MD5. Esto significa que entre cliente y servidor radius se usará cifrado MD5 en la autenticación EAP.

Configuración en el portátil

En el portátil hay que activar 802.1X para que el portátil realice la autenticación. Esto se hace en 'Desktop > IP Configuration', donde hay que activar 'Use 802.1X Security' y configurar un usuario y contraseña que esté dado de alta en el Radius.

Comprobación del funcionamiento

Podemos comprobar el funcionamiento de 802.1X activando el modo simulación, y habilitando en el filtro de protocolos Radius y EAPoL. Si conectamos el PC del intruso podremos ver cómo se rechaza la autenticación, y si conectamos el PC de Pepe, veremos cómo el servidor Radius autoriza su conexión.

5. RIP y EIGRP

5.1 Objetivo

El objetivo de esta práctica es aprender a configurar en una red modular jerárquica de routers Cisco dos protocolos de enrutamiento dinámico de vector de distancias: RIPv1, RIPv2 y EIGRP.

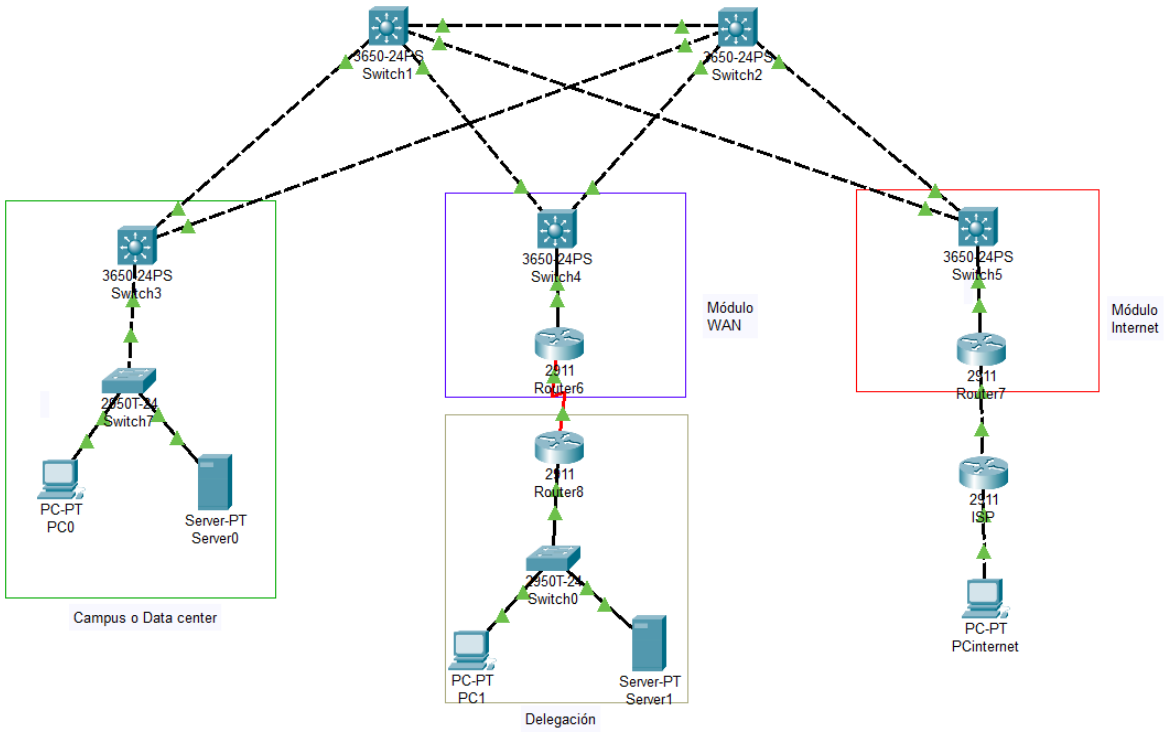
5.2 Competencias

Tras la finalización de la práctica deberían haberse adquirido las siguientes competencias:

- Conocer las características principales y el funcionamiento básico de RIPv1, RIPv2 y EIGRP.
- Conocer las limitaciones de protocolos de enrutamiento classful, como RIPv1, en subredes discontiguas.
- Saber cómo configurar RIPv1, RIPv2 y EIGRP en una red modular jerárquica de routers Cisco.
- Saber cómo configurar una ruta por defecto y anunciarla mediante RIP y EIGRP.
- Saber cómo sumarizar rutas en EIGRP.

5.3 Configuración de enrutamiento dinámico en red modular jerárquica

En este laboratorio vamos a configurar enrutamiento dinámico en la siguiente red:



5.4 RIP

Como ya sabemos, hay dos versiones del protocolo RIP:

- RIPv1: Es la versión más antigua de RIP. Es classful, o lo que es lo mismo, sólo es capaz de trabajar con las clases por defecto de las direcciones IP, no soporta máscaras de subred. Esto es una limitación en redes donde se usan subredes no contiguas, ya que en estos casos RIP no sería capaz de enrutar el tráfico, ya que sólo podría guardar una ruta a la red correspondiente a la clase (por ejemplo, 10.0.0.0, 192.168.1.0).
- RIPv2: Versión mejorada de RIP. Es classless, o lo que es lo mismo, soporta máscaras de subred. Esto es a consecuencia de añadir varios campos en la tabla de encaminamiento que se intercambian los routers, entre ellos, la máscara.

En esta práctica empezaremos configurando la versión por defecto en Cisco de RIP, que es RIPv1, y que ya sabemos configurar.

5.4.1 Configuración de RIPv1

RIPv1 es la versión de RIP por defecto en Cisco. Podemos configurarla como ya hemos hecho otras veces, usando la interfaz gráfica de packet tracer. En cada router o multilayer switch en Config > RIP. Tendríamos que añadir las redes directamente conectadas a cada equipo, es decir, las redes a las que pertenecen sus interfaces. Como es un protocolo classful, automáticamente sumarizará (resumirá) a la clase a la que pertenece la red. Por ejemplo, si tenemos en una interfaz la IP 10.1.0.5/30, en RIPv1 resumirá a la red 10.0.0.0, ya que al empezar por "10." es clase A.

La configuración vía interfaz gráfica es equivalente a la siguiente configuración vía CLI:

```
Router(config)#router rip
Router(config-router)#network [red_directamente_conectada]
```

Configuraremos RIP en todos los routers y multilayer switches de la red. Como excepción, **no incluiremos en RIP en Router7 la subred de la interfaz conectada a internet**, ya que esta subred es externa y conviene no anunciarla hacia la red interna. Más adelante configuraremos una ruta por defecto para la conectividad con internet.

Una vez configuremos RIP en todos los routers y multilayer switches podemos ver **que no hay conectividad entre los PCs**, por ejemplo, entre los del Campus y los de la delegación. Ejecutando los siguientes comandos podemos ver que esto es debido a que Switch3 y Switch4 ven la red 10.0.0.0/8 y la anuncian a Switch1 y Switch2, y éstos enrutarán todo el tráfico a dicha red hacia Switch3, por tener menos coste.

```
Switch#sh ip route
Switch#show ip rip database
Switch#debug ip rip          #Activa los logs de modo debug de RIP
```

El último comando activa un debug. **Este comando en una red en producción con tráfico real es extremadamente peligroso** y únicamente debe utilizarse en casos extremos, a ser posible en horas de bajo tráfico, y con supervisión de los administradores de red. Los debugs pueden generar mensajes de logs masivos, que pueden impedir introducir más comandos, e incluso colapsar el router, haciendo que éste deje de procesar tráfico. Sin embargo, en un entorno de laboratorio es un comando muy útil para entender el funcionamiento de los equipos.

Para parar el debug hay que introducir el siguiente comando:

```
Switch#undebug all        #Desactiva todos los debugs
```

El comando anterior también funciona escribiendo sólo ' u all' o 'u al', y algunas veces salen tantos logs que no nos dejan escribir el comando completo, y es conveniente usar alguno de estos últimos.

5.4.2 Configuración de RIPv2

RIPv2 se configura igual que RIPv1. Tan solo hay que añadir el comando 'version 2' en el nivel de configuración 'router rip'. También conviene evitar que el router realice sumarización automática a la clase, con el comando 'no auto-summary', para evitar el problema que ya hemos visto de subredes discontiguas. La configuración en este caso sólo puede ser vía CLI, aunque las redes (comando 'network ...') no hace falta volverlas a configurar, porque ya están del paso anterior.

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto-summary
Router(config-router)#network [red_directamente_conectada]    #No es
necesario configurar las redes de nuevo
```

Una vez configuremos RIPv2, veremos como ya funciona la conectividad entre los PCs de la sede central y de la delegación, y en las tablas de rutas ya aparecen las subredes correctamente.

> **Nota:** Un error típico es olvidar en algún router incluir el comando 'version 2'. Si se nos olvida, este router no anunciará subredes y algo no funcionará.

Ahora configuraremos una **ruta por defecto hacia internet** en el router de acceso a internet (Router7) y la anunciaremos en RIP para que la vean el resto de routers de la red. Para anunciar una ruta por defecto en RIP, se configura una ruta estática por defecto, y se redistribuye en rip con el comando 'default information originate' en el nivel de configuración 'router rip'. Una vez configurado esto podremos hacer ping desde un PC de la central o la delegación al PC de internet.

```
Router(config)#ip route 0.0.0.0 0.0.0.0 [IP_o_interfaz_destino]
Router(config)#router rip
Router(config-router)#default-information originate
```

Es importante que, por norma general, salvo que se quiera hacer por alguna razón concreta, **no se anuncie RIP hacia redes externas** (como por ejemplo en la salida hacia Internet), **ni hacia los switches de la capa de acceso**. Para ello se usa el comando 'passive-interface':

```
Router(config)#router rip
Router(config-router)#passive-interface [interfaz]
```

Puede encontrarse más información sobre cómo configurar RIP en: freeccnastudyguide Apartado 5.2

5.5 EIGRP

En los siguientes recursos puede encontrarse un buen resumen del protocolo EIGRP y cómo configurarlo:

- freeccnastudyguide - Apartado 5. EIGRP
- freeccnastudyguide - Apartado 5.5. Configuring EIGRP

Para configurar EIGRP lo ideal es seguir los siguientes pasos:

1. Dividir la red que queremos configurar en sistemas autónomos. Los routers establecerán relaciones de vecinos en EIGRP sólo dentro de cada sistema autónomo. En nuestro caso, podemos usar un único número de sistema autónomo para toda la red. El identificador de sistema autónomo tendremos que incluirlo en el comando de configuración 'router eigrp <AS>'. Tendrá que ser el mismo identificador en los routers si queremos que éstos compartan las rutas.
2. En cada router en que queramos activar EIGRP, configuraremos las redes directamente conectadas que queremos anunciar. Esto se hace con el comando de configuración 'network ...', como en RIP, en este caso añadiendo un wildcard de máscara opcional (ojo, un wildcard, como en las ACLs), para incluir en EIGRP sólo algunas de las interfaces si lo necesitásemos. En nuestro caso no nos hace falta. También, al igual que RIPv2, evitamos la autosumarización a la clase.
3. Desactivamos anuncios de EIGRP en las interfaces en donde no queremos que se envíen mensajes EIGRP. Por ejemplo, en interfaces externas de la red (como en la interfaz de salida hacia Internet). Esto se hace con el comando de configuración 'passive-interface', de forma similar a RIP.

```
Switch(config)#router eigrp [AS]
Switch(config-router)#network [red_directamente_conectada]
Switch(config-router)#no auto-summary
Switch(config-router)#passive-interface [interfaz]
```

4. Creamos ruta(s) por defecto para la salida a internet y la redistribuimos a eigrp. Esto se hace (en el router de salida a internet, Router7):

```
Router(config)#ip route 0.0.0.0 0.0.0.0 [IP_o_interfaz_destino]
Router(config)#router eigrp [AS]
Router(config-router)#redistribute static metric 100000 1000 255
1 1500
```

5. Sumarizamos. Para sumarizar se utiliza el comando de configuración 'ip summary-address eigrp ...' **a nivel de interfaz**.

   Importante: En función de la versión de IOS (el O.S. de cisco), puede que esté habilitado por defecto la auto-sumarización a la clase. Si éste es el caso, hay que

desactivarla en la configuración a nivel de 'router eigrp' con el comando 'no auto-summary' para que nos funcione bien la sumarización a subredes (la recomendación es hacerlo siempre por si acaso).

a. Sumarización *distribución -> core*. En routers de distribución hay que enviar hacia el core sólo ruta(s) de resumen.

   El siguiente ejemplo muestra cómo sumarizar en Switch3 las rutas del Campus, de forma que se anuncie hacia el core sólo la red 10.0.0.0/16.

```
Switch#conf t
Switch(config)#interface gi1/0/1
Switch(config-if)#ip summary-address eigrp 1 10.0.0.0
255.255.0.0
Switch(config-if)#interface gi1/0/2
Switch(config-if)#ip summary-address eigrp 1 10.0.0.0
255.255.0.0
```

b. Sumarización *core -> distribución*. Lo ideal sería filtrar (no enviar) en los anuncios EIGRP las rutas intermedias de las interfaces, tanto en *distribución -> core* como en *core -> distribución*, de tal forma que los routers de distribución sólo vean las redes sumarizadas, y no las subredes correspondientes a las interfaces del core. Sin embargo, para ello haría falta utilizar el comando 'distribute-list', que no está implementado en packet tracer. Lo que sí que podemos hacer es sumarizar en los routers de core para enviar a los routers de distribución sólo una super-red (lo contrario a subred) que incluya las subredes de todas las interfaces del core.

   El siguiente ejemplo muestra cómo se sumarizaría en Switch1 los anuncios a Switch3, enviando una única ruta para la super-red 192.168.0.0/16, en lugar de múltiples rutas para cada subred dentro del /16.

```
Switch#conf t
Switch(config)#int gi1/0/2
Switch(config-if)#ip summary-address eigrp 1 192.168.0.0
255.255.0.0
```

Nota: Al sumarizar en eigrp, en la tabla de rutas del router donde sumarizamos aparece la ruta sumarizada enviada a null0. Si en ese router no hay rutas más específicas que correspondan a la red sumarizada, todo lo que le llegue a la red sumarizada lo descartará. Esto puede ocurrir por ejemplo si sumarizamos a la misma red en dos routers conectados entre sí, y uno de ellos aprende del otro por EIGRP todas las rutas más específicas de la red sumarizada.

6. Comprobamos que todo funciona bien. Los comandos para comprobar que todo está bien configurado son el ya conocido 'show ip route' para ver la tabla de rutas, y también todos los comandos que están bajo 'show ip eigrp ...'. Podemos ver todas las opciones con la ayuda del CLI (la '?'):

```
Switch#show ip route
Switch#show ip eigrp ?
  interfaces  IP-EIGRP interfaces
  neighbors   IP-EIGRP neighbors
  topology    IP-EIGRP Topology Table
  traffic     IP-EIGRP Traffic Statistics
```

7. Para pensar un poco: Reflexionad si es necesario configurar RIP/EIGRP en los Routers 7 y 8, y qué ventajas e inconvenientes tiene hacerlo con respecto a usar rutas estáticas.

6. OSPF

6.1 Objetivo

El objetivo de esta práctica es aprender a configurar en una red modular jerárquica de routers Cisco el protocolo de enrutamiento dinámico de estado de enlace OSPF.

6.2 Competencias

Tras la finalización de la práctica deberían haberse adquirido las siguientes competencias:

- Conocer las características principales y el funcionamiento básico de OSPF.
- Conocer cuál es el papel en una red OSPF de los ABRs y ASBRs.
- Saber cómo configurar OSPF multiárea en una red modular jerárquica de routers Cisco.
- Saber cómo configurar una ruta por defecto y anunciarla mediante OSPF.
- Saber cómo sumarizar rutas en OSPF.

6.3 Enlaces de interés

En los siguientes recursos puede encontrarse un buen resumen del protocolo OSPF y cómo configurarlo:

- freeccnastudyguide - Apartado 5. OSPF
- freeccnastudyguide - Apartado 5.8. Configuring OSPF

Otra buena explicación de OSPF multiárea:

Configuración de OSPF Multiárea - ccnadesdecero

También Cisco tiene abundante documentación que explica el diseño, funcionamiento y configuración de OSPF, como por ejemplo:

- OSPF Design Guide - Cisco
- Designing Scalable OSPF Design

Explicación de los tipos de anuncios de routing y tipos de áreas en OSPF:

- OSPF LSA Types - ipcisco

6.4 Configuración de OSPF en una red modular jerárquica

OSPF es un protocolo de routing jerárquico, que divide una red en áreas. Siempre tiene que haber un área 0, que es el backbone OSPF, a la cual se interconectan el resto de áreas. Los routers que forman parte de más de un área se denominan ABR. Los routers que importan rutas de dominios no-OSPF se denominan ASBRs.

Lo primero que tendremos que hacer, antes de configurar OSPF, es realizar una topología de la red indicando en ella las áreas OSPF, los ABRs y los ASBRs. En un diseño modular jerárquico, la estructura general que podemos seguir es hacer que el Core sea el área 0, y los distintos módulos sean áreas distintas. Situaremos los ABRs en los routers de distribución, para liberar a los routers del core de la carga de ser ABRs, ya que un ABR mantiene una base de datos de cada área. Por lo tanto, a nivel general una topología modular jerárquica dividida en áreas OSPF sería similar a la siguiente:

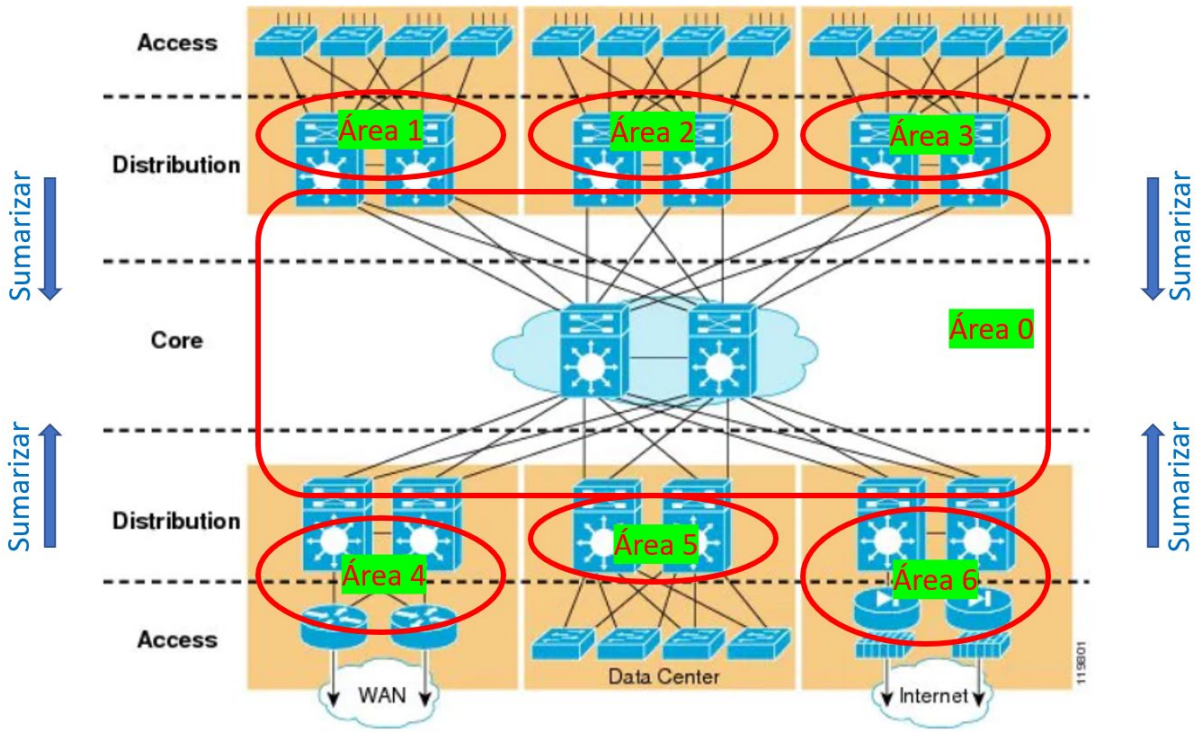


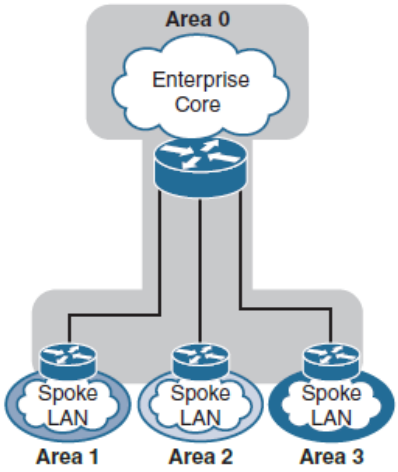
Imagen creada a partir de la siguiente fuente: Cisco. Campus Network for High Availability Design Guide. May 21, 2008.
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html

Sobre esta topología hay que hacer una precisión con respecto a los módulos que agregan la interconexión con otras redes internas de la organización, como son el módulo WAN y el módulo de VPNs. En OSPF todas las áreas tienen que estar conectadas al Core, por lo que no podemos ubicar, por ejemplo, el módulo WAN en un área distinta del 0, y el módulo de una delegación (Branch) en otra área, ya que esta última no estaría conectada con el área 0. Debido a ello, tenemos varias opciones. La que escojamos dependerá del diseño de red y los requisitos.

- El módulo remoto (por ejemplo, la delegación) tiene su propio dominio de routing y no forma parte del dominio OSPF del core de la organización. La comunicación a nivel de routing entre el módulo WAN y el módulo remoto tendría que ser o bien mediante

enrutamiento estático, o bien usando BGP (esto último queda fuera del alcance de la asignatura).

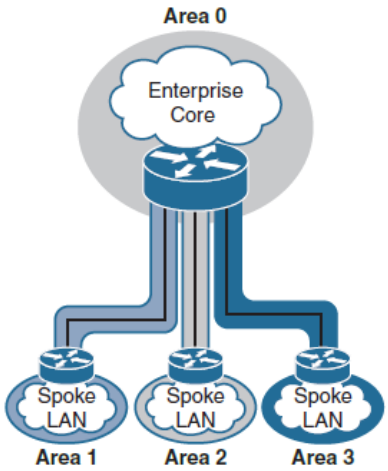
- Extender el área 0 hasta el router edge (frontera) del módulo remoto (de la delegación), que sería un ABR. Esto implica que extenderíamos el área 0 a todos los módulos remotos, y por lo tanto, las rutas de los módulos remotos se verían en el core y en el resto de módulos remotos. Esto afectaría al tiempo de convergencia, y la inestabilidad en un módulo remoto podría afectar al resto.



Fuente: Marwan Al-shawi, André Laurent. Designing for Cisco Network Service Architectures (ARCH) Foundation Learning Guide, Fourth Edition CCDP ARCH 300-320. Cisco Press. 2017

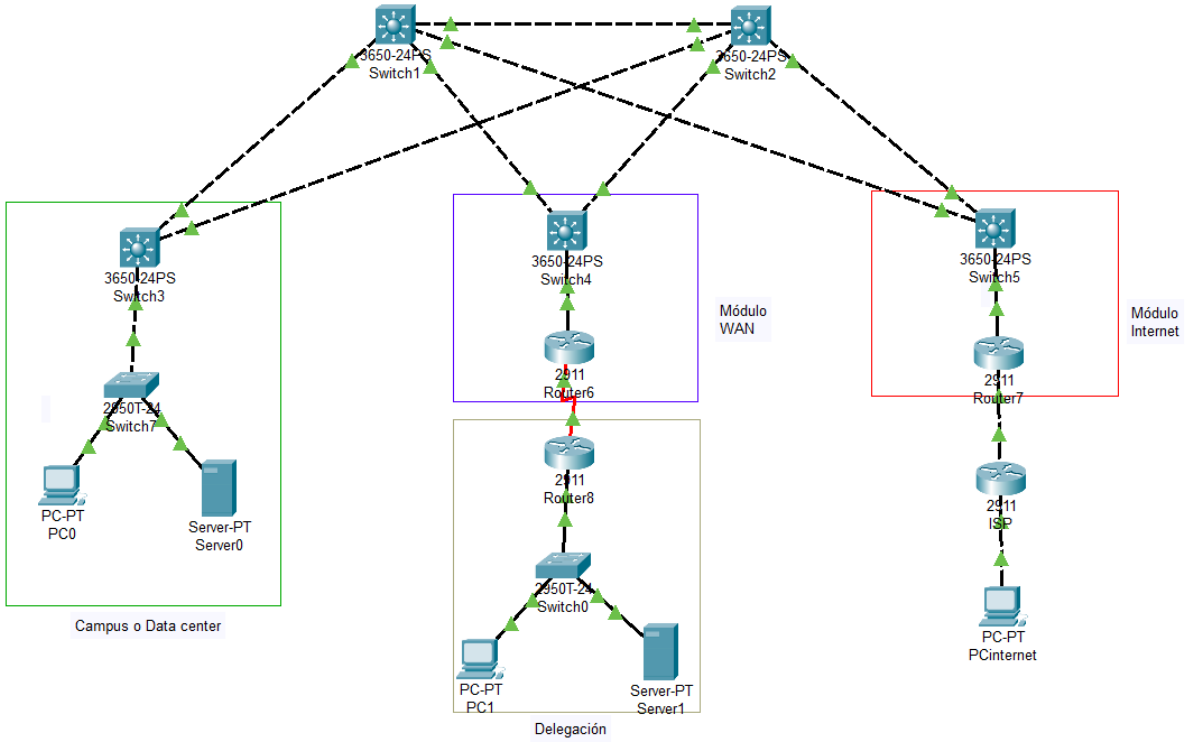
- Extender el área 0 sólo hasta el router concentrador de módulos remotos (concentrador de VPNs o WANs). Este router sería un ABR, y formaría parte del área 0, y de la(s) área(s) de los módulos remotos. Esta solución tiene el inconveniente de que el ABR pertenecería a varias áreas, y tendría que mantener una base de datos de cada área. Es importante que este router tenga potencia suficiente para soportar esto, no serviría cualquier router. La recomendación de Cisco en routers antiguos es que un ABR pertenezca a un máximo de 3 áreas. Actualmente hay routers muy potentes que pueden soportar decenas de áreas (también dependerá del tipo de áreas, cantidad de routers y rutas, etc). Dentro de esta opción tendríamos a su vez varias opciones.
    - Ubicar todos los módulos remotos en la misma área.
    - Ubicar cada módulo remoto en un área distinta
    - Una solución intermedia, en la que establecemos áreas que son compartidas por varios módulos remotos.

En nuestro caso, para simplificar, y ya que no vamos a manejar muchas delegaciones y éstas van a tener pocos routers y subredes, podemos suponer que el router concentrador del módulo WAN o VPN tiene potencia suficiente, y definir que éste será el ABR, y cada módulo remoto pertenecerá a un área distinta. En todo caso, si se detectasen problemas en la convergencia o eficiencia del router ABR, la solución sería meter todos los módulos remotos en la misma área.

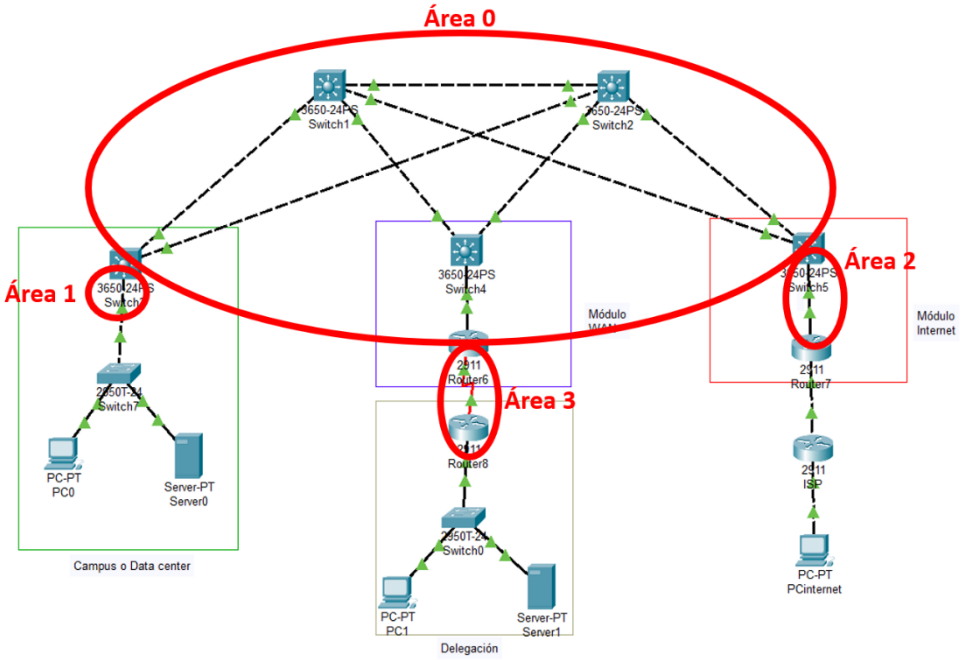


Fuente: Marwan Al-shawi, André Laurent. Designing for Cisco Network Service Architectures (ARCH) Foundation Learning Guide, Fourth Edition CCDP ARCH 300-320. Cisco Press. 2017

En este laboratorio vamos a configurar OSPF en la siguiente red:



Siguiendo las recomendaciones anteriores para la topología de áreas de una red OSPF, podemos definir por ejemplo las siguientes áreas en esta red:



Viendo la imagen anterior, trata de identificar cuáles son los ABRs y ASBRs de la red.

Una vez hemos definido la topología OSPF, los pasos para configurar el enrutamiento OSPF serían los siguientes:

1. Crear, si no está ya, en los routers que hablarán OSPF una interfaz de loopback (interfaz lógica interna) y asignarle dirección IP. Esta interfaz será la que usará OSPF para identificar cada router en la topología.
2. En cada router en que queramos activar OSPF, incluiremos en OSPF las redes directamente conectadas a las que pertenecen los enlaces que queremos anunciar. Esto se configura con el comando 'network ...', como en RIP y EIGRP, en este caso añadiendo un wildcard de máscara (ojo, un wildcard, como en las ACLs) e indicando también el área al que pertenecen las interfaces de esa red. Esto se hace en el nivel de configuración 'router ospf [*pid*]', donde [*pid*] es el identificador numérico del proceso ospf, que es local a cada router para poder activar más de un proceso de routing. No tiene por qué ser el mismo en distintos routers, aunque se recomienda que sí lo sea para mayor claridad.

```
Switch(config)#router ospf [pid]
Switch(config-router)#network [IP] [wildcard] area [area_id]
```

A medida que se va activando OSPF e incluyendo en OSPF las redes, es bueno ir comprobando que se establecen las relaciones de vecinos entre los routers, para darnos cuenta si hemos cometido algún error. Esto se hace con el siguiente comando.

```
Switch#show ip ospf neighbor
```

Una vez hayamos configurado OSPF en todos los routers e incluidos las redes en OSPF, ya deberíamos tener conectividad entre los PCs del Campus y de la delegación. También podemos comprobar que las tablas de rutas muestran las rutas aprendidas por OSPF.

3. En cada router, configuraremos las interfaces en las que no queremos que se envíen mensajes OSPF como pasivas. Éstas serán las interfaces contra redes externas (por ejemplo, en el router de acceso a internet, la interfaz contra el ISP), y las interfaces en routers de distribución contra switches de acceso que no hablan OSPF.

```
Switch(config)#router ospf [pid]
Switch(config-router)#passive-interface [interfaz]
```

4. Configuramos en el router de acceso a internet una ruta por defecto y la redistribuimos a OSPF. Podemos comprobar si la ruta por defecto se ha propagado bien viendo si aparece en las tablas de rutas del resto de routers.

```
Router(config)#ip route 0.0.0.0 0.0.0.0 [IP_o_interfaz_destino]
Switch(config)#router ospf [pid]
Router(config-router)#default-information originate
```

5. Sumarización. En OSPF sólo se puede sumarizar en ABRs.
    a. Sumarización sentido *core -> distribución*

    En el ABR del módulo de internet sumarizamos las subredes que se anuncian hacia el área del módulo de Internet. Para ello se utiliza el comando de configuración 'area [*id*] range...', donde indicaremos las redes sumarizadas que se anuncian desde el área 0 hacia el módulo de Internet (se pueden usar varios comandos si queremos configurar varias redes resumen).

```
Switch(config)#router ospf [pid]
Router(config-router)#area 0 range [IP] [máscara]
```

Nota: *En la versión actual de Packet Tracer no siempre funciona bien este último comando, y puede que no propague bien la ruta resumen.*

Para el resto de áreas que no son las del módulo de internet, que no tienen conexión con otras redes no-OSPF, podemos definir estas áreas de tipo *totally stub*. El ABR de un área *totally stub* no dejará pasar ninguna ruta desde el backbone, y enviará hacia el área *totally stub* una ruta por defecto (puede verse aquí un pequeño resumen de los tipos de área OSPF). Esto hay que configurarlo en todos los routers que hablen OSPF del área, ya que en los mensajes hello va incluido el tipo de área, y si no coincide no levanta la relación de vecinos.

```
Switch(config)#router ospf [pid]
Router(config-router)#area [area_id] stub no-summary
```

b. Sumarización en sentido *distribución -> core*:

En los ABRs de las áreas que no son el módulo de internet (ya que en éste estamos enviando una ruta por defecto hacia el core y no es necesario sumarizar) se sumariza con el siguiente comando, indicando la red resumen (se pueden usar varios comandos si queremos configurar varias redes resumen).

```
Switch(config)#router ospf [pid]
Router(config-router)#area [area_id] range [IP] [máscara]
```

Nota: *En la versión actual de Packet Tracer no siempre funciona bien este último comando, y puede que no propague bien la ruta resumen.*

6. Comprobación y troubleshooting. Además de realizar pings entre los distintos hosts, los siguientes comandos permiten ver el estado y funcionamiento de OSPF:

```
Switch#sh ip route          #IP routing table
Switch#show ip protocols    #IP routing protocol process
parameters and statistics
Switch#sh ip ospf ?
  <1-65535>       Process ID number
  border-routers  Border and Boundary Router Information
  database        Database summary
  interface       Interface information
  neighbor        Neighbor list
  <cr>
```

Nota importante: Cada vez que cambiamos algo relevante en la configuración OSPF de un router, como las redes a las que pertenecen las interfaces que se anuncian, el tipo de área, o se sumariza, puede que el proceso OSPF no se actualice bien y no aparezca en la tabla de rutas todo lo que debería (esto suele pasar en la sumarización del módulo de internet). Si esto ocurre, conviene reiniciar el proceso OSPF en el router:

```
Router#clear ip ospf process
Reset ALL OSPF processes? [no]: yes
```

O incluso reiniciar el router, o los dos routers involucrados simultaneamente (antes de hacerlo, guardar la configuración con el comando 'wr mem'):

```
Router#wr mem               #Equivalente a 'copy running-config
startup-config'
Router#reload
```

7. Gestión de red

7.1 Objetivo

El objetivo de esta práctica es aprender las nociones básicas de la gestión de una red, y cómo configurarlas en una red pequeña con dispositivos Cisco.

7.2 Competencias

Tras la finalización de la práctica deberían haberse adquirido las siguientes competencias:

- Conocer los tipos de gestión en banda y fuera de banda, sus implicaciones, y algunos escenarios en que usar cada tipo de gestión
- Conocer el rol de un Sistema de Gestión de Red (NMS).
- Conocer la utilidad de tecnologías habituales que se usan en la gestión de una red, como snmp, syslog, ntp, y netflow, y cómo configurarlas en una red Cisco sencilla.
- Comprender el propósito de los distintos puertos de gestión que puede tener un dispositivo de red, como los puertos de consola, auxiliar, gestión, o un puerto de red normal, y saber cómo configurarlos en una red.
- Conocer para qué sirve un servidor de terminales, y cómo configurar uno para el acceso remoto a puertos de consola de equipos de red.
- Saber cómo realizar la configuración básica en routers y switches Cisco de acceso a los mismos incluyendo distintos tipos de autenticación (local y radius), banner de bienvenida, acceso ssh y por consola.
- Comprender la necesidad de proteger una red de gestión, y realizar una configuración básica de filtros de seguridad que permita proteger una red de gestión de una red sencilla.

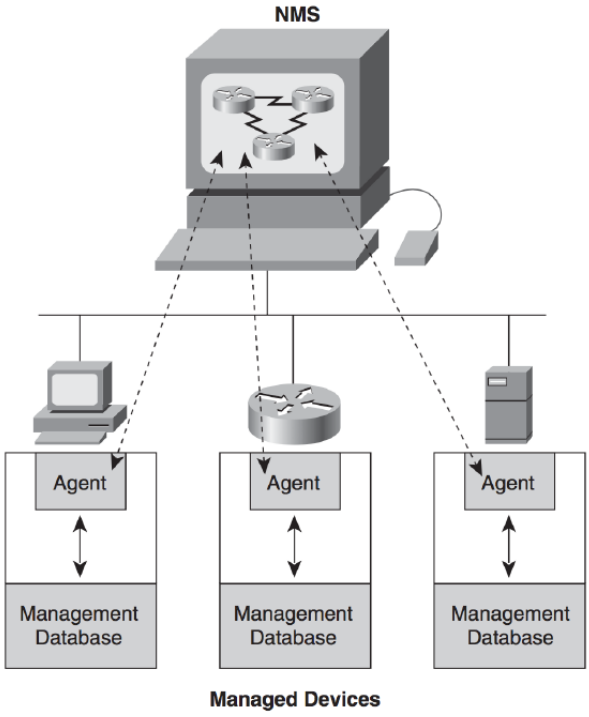
7.3 Enlaces de interés

- Cisco SAFE Reference Guide. Chapter 9: Management
- ¿Cómo configurar NTP en Cisco?
- syslog: Funcionamiento y Configuración
- NetFlow: Funcionamiento y Configuración
- SNMP: Funcionamiento y Configuración
- Configuring Secure Shell on Routers and Switches Running Cisco IOS
- Management Port vs Console Port in Networking Devices
- CAB-OCTAL-ASYNC Cable Pinouts
- Configuring the Terminal Server
- Configuring a Terminal/Comm Server

7.4 Gestión de red

Gestión de red es el conjunto de funciones para controlar, planificar, reservar, desplegar, coordinar y monitorizar recursos en una red de computadores. La ISO define un modelo de gestión FCAPS de red, donde la gestión estaría formada por procesos de gestión de Fallos, Configuración, contabilidAd, desemPeño y Seguridad. Una red debe tener los mecanismos necesarios que permitan realizar de forma eficiente, la configuración de la misma, la monitorización de su estado y funcionamiento, y la resolución de problemas que puedan ocurrir.

Por norma general la arquitectura de gestión de red consiste en **dispositivos gestionados** (routers, switches, servidores, etc), **un sistema de gestión de red (NMS)** que se comunica con los dispositivos y proporciona al usuario información del estado de la red, y un software que corre en cada dispositivo de red, llamado **agente**, que es con quien se comunica el NMS, y que entre otras cosas, se encarga de recopilar información del dispositivo y enviársela al NMS.



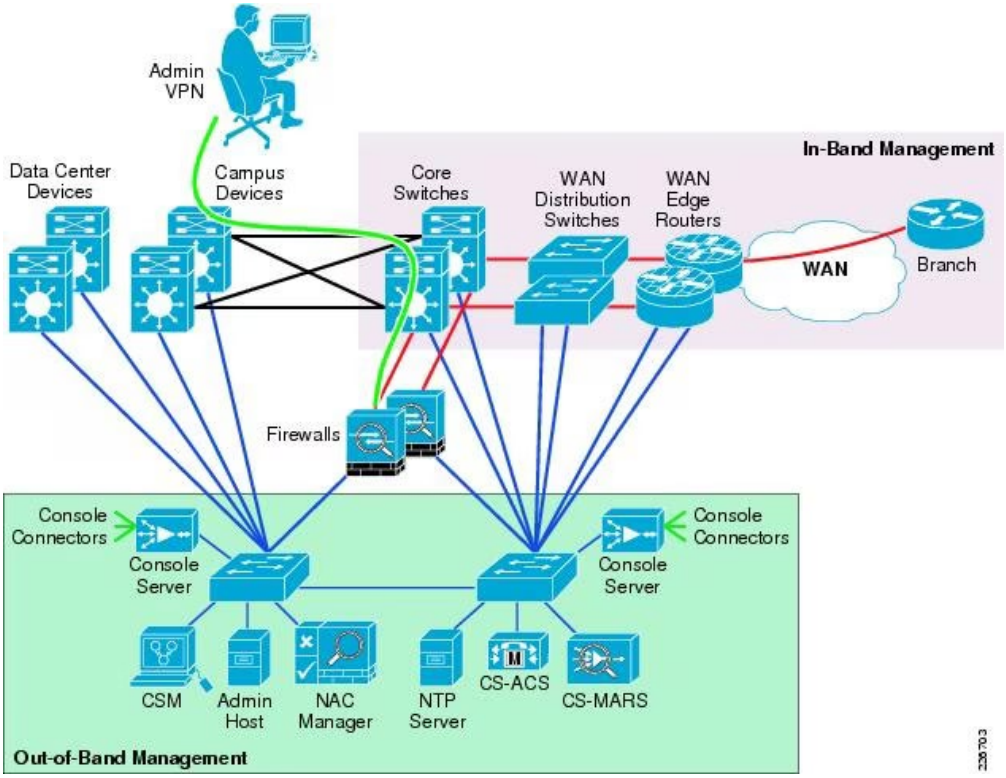
Fuente: Priscilla Oppenheimer. Top-Down Network Design. Third Edition. Cisco Press. 2011

7.5 Tipos de gestión de red

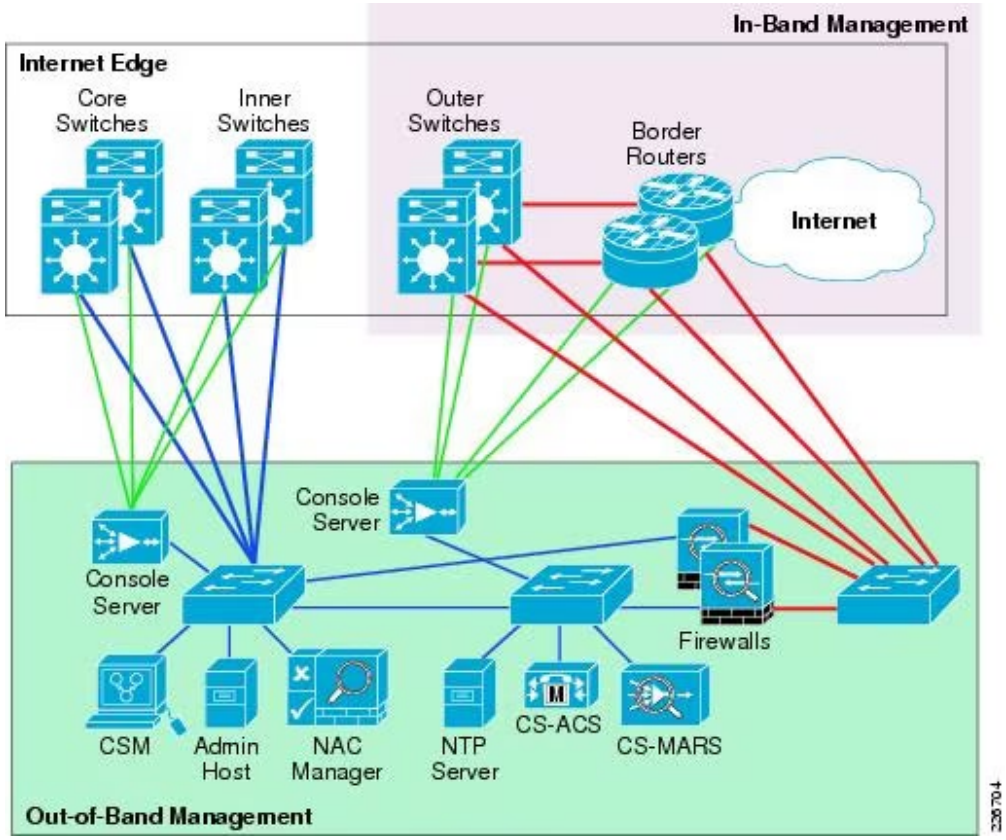
Si todos los NMSs están ubicados en un área de la red, normalmente un NOC (network operations center) o NMC (network management center), hablamos de que hay una gestión **centralizada**. Pero también puede ocurrir que los NMSs estén **distribuidos** a lo largo de la red, o que formen una estructura **jerárquica**, con un NMS central, gestor de gestores, y otros NMSs dedicado cada uno a tareas específicas.

Por otro lado, la gestión de una red puede ser **en banda**, si los datos de gestión usan los mismos circuitos y dispositivos que el tráfico de los usuarios (tráfico de servicio), o **fuera de banda**, si se usan circuitos y dispositivos dedicados a gestión, distintos que los de servicio. Una gestión fuera de banda generalmente implica una red dedicada a la gestión, denominada 'red de gestión'. En redes medianas o grandes suele existir una red de gestión, con sus propios dispositivos (routers, switches, etc), que puede ser bastante grande. Debido a que la red de gestión tiene acceso a todos los dispositivos y NMSs, suele ser una red altamente protegida y muy restringida, a la que sólo puede acceder usuarios específicos, como administradores, ingenieros de sistemas, o ingenieros de soporte de red. También suele ser una red aislada de la red de servicio, de manera que desde la red de gestión sólo puede accederse a las interfaces o IPs de gestión de la red de servicio, y sólo debe permitirse el tráfico específico de los protocolos de gestión usados.

En redes medianas o grandes que siguen la arquitectura SAFE de Cisco puede utilizarse una combinación de gestión en banda y fuera de banda. Se realiza una gestión fuera de banda dentro de la sede central de la organización, y se realiza gestión en banda de los equipos de las delegaciones. También se realiza gestión en banda de los equipos del módulo de internet que estén más allá del firewall, por ejemplo, del router de acceso a internet. De manera general siempre hay que proteger mediante un firewall el acceso a la red de gestión de dispositivos que estén expuestos a internet o a otras redes.



Fuente: Cisco. Cisco SAFE Reference Guide. Cisco Validated Design. OL-19523-01. July 8, 2010



Fuente: Cisco. Cisco SAFE Reference Guide. Cisco Validated Design. OL-19523-01. July 8, 2010

En redes grandes puede haber incluso varias subredes de gestión fuera de banda, en VLANes distintas, como por ejemplo una para las consolas, otra para realizar los backups (ya que éstos pueden requerir mucho ancho de banda en momentos puntuales), y otra para el resto de tareas de gestión.

7.6 Puertos de gestión

Los dispositivos de red suelen incorporar **puertos especiales para la gestión** de los mismos fuera de banda:

- **Puerto de consola**. Es un puerto serie que incluyen la mayoría de proveedores de equipos de redes. En el caso de Cisco, Juniper, y muchos otros, es un puerto serie asíncrono RS-232 (EIA/TIA-232) con conector de varios tipos, como RJ-45, DB-25 o USB. Generalmente requiere una configuración concreta en el otro extremo para que funcione la conexión serie, como por ejemplo (hay que consultar la documentación del dispositivo concreto):
  9600 baudios
  8 bits de datos
  Sin paridad
  1 bit de parada

El puerto de consola es el que se utiliza para la configuración inicial del dispositivo, y para el acceso al mismo cuando conectarse a él mediante un puerto normal de servicio o de gestión con IP no es posible por la razón que sea. También permite un acceso fuera de banda al equipo.
Antiguamente los ordenadores tenían un puerto serie con conector DB-9, y el cable más usado para la conexión de un ordenador a un puerto de consola era un cable con conector DB-9 en un extremo y RJ-45 en el otro. Posteriormente, los portátiles eliminaron el puerto serie y había que utilizar un cable USB a DB-9 y otro cable "de consola", es decir, DB-9 a RJ-45. Más tarde aparecieron cables USB a RJ-45, y ya hace años que los dispositivos tienen puertos de consola con conector USB. En algunas ocasiones hay varios conectores para el mismo puerto de consola (por ejemplo, un RJ-45 y un mini-USB), pero sólo se puede usar uno de ellos al mismo tiempo.

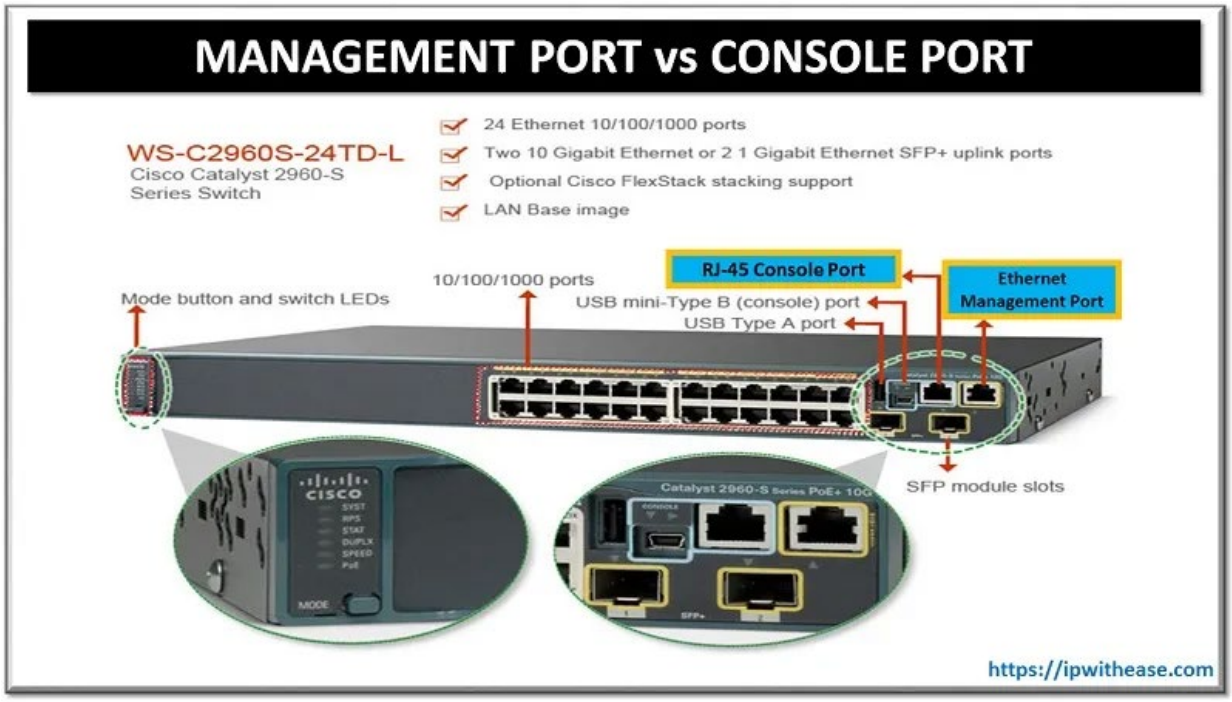
Cisco - CAB-CONSOLE-RJ45= - Console Cable 6...
tonitrus.com · En stock

HDE USB to Serial Interface Cable with Serial t...
amazon.es

Cisco - CAB-CONSOLE-USB= - Console Cable 6 f...
tonitrus.com · En stock

- **Puerto auxilar (AUX)**. Es similar al de consola. Muchos equipos incluyen un puerto de consola y un auxiliar para permitir que uno esté permanente conectado con un cable para el acceso remoto al puerto de consola, y el otro quede libre para poderse conectar en local al equipo.
- **Puerto de gestión**. Es un puerto ethernet con conector RJ-45 al que se le puede configurar una IP y acceder remotamente con ssh o telnet. Este puerto suele estar aislado en hardware o software del resto de puertos de servicio, de manera que es un puerto fuera de banda seguro, sin comunicación posible con los demás. Un puerto de este tipo facilita la conexión remota fuera de banda al dispositivo.

Además de estos puertos especiales, puede usarse **cualquier otro puerto libre** como puerto de gestión, pero en este caso, si se desea un acceso fuera de banda, es necesario securizar este puerto con ACLs para aislarlo de los de servicio, y en el caso de routers, configurarlo pasivo, para que no anuncie rutas, y evitar que la subred de gestión sea anunciada por los protocolos de routing a otros routers.

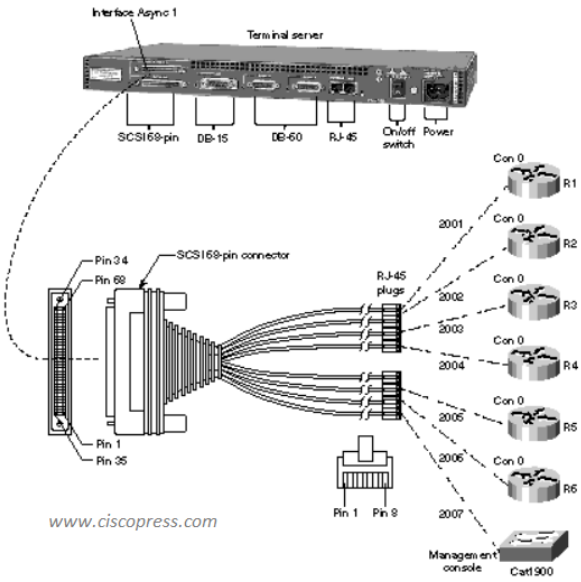


7.7 Servidor de terminales

El acceso remoto a un puerto de servicio dedicado a gestión o a un puerto de gestión es sencillo, ya que sólo hay que configurarle una IP, permitir el acceso por telnet o ssh (mejor ssh por seguridad), y dar conectividad a esa IP. Sin embargo, en un puerto serie RS-232 no puede configurarse una dirección IP. Debido a ello, suele montarse otro dispositivo cerca, que sí tiene IP, éste se cablea con un cable serie al puerto de consola, y el acceso remoto se realiza al dispositivo que tiene IP, y éste se conecta con la conexión serie al que queremos gestionar. Como por norma general habrá varios equipos de red en el mismo rack o CPD, suele montarse un dispositivo con muchos puertos serie, a través del cuál podemos conectarnos remotamente al puerto de consola de los equipos de red. Dicho dispositivo se suele denominar servidor de terminales (*terminal server*), y puede tener muchos puertos serie con conector RJ-45, cada uno para conectarse a la consola de un equipo de red. Si el dispositivo es un router también se le denomina router de consolas.

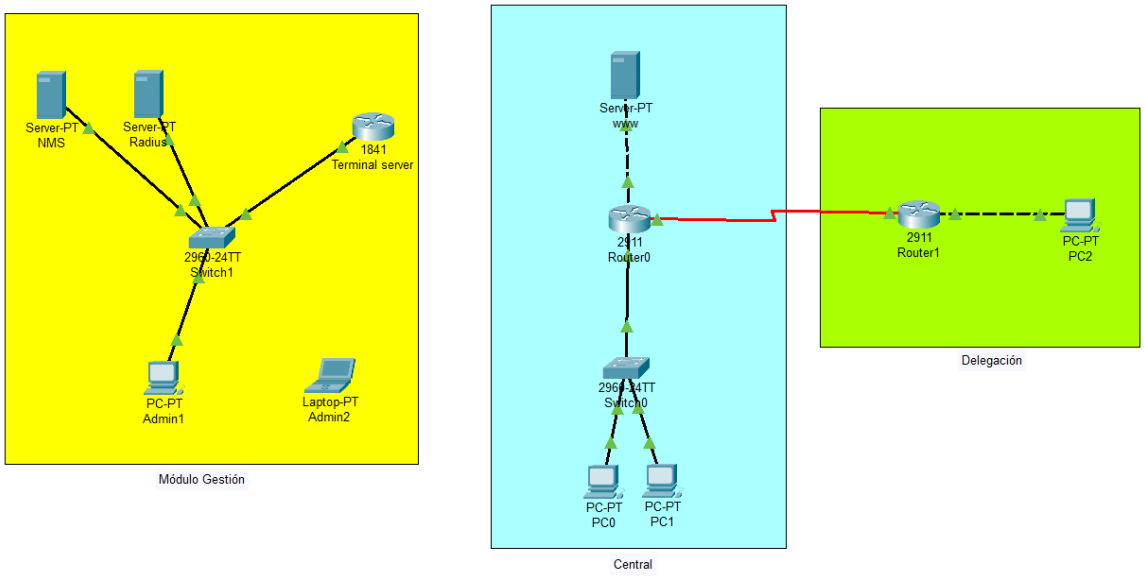
Fuente: https://networklessons.com

El servidor de terminales también puede montar un puerto serie SCSI-68 (o varios), del que pueden salir 8 cables RJ-45, uno para la consola de cada dispositivo. El cable que conecta de un SCSI-68 a múltiples consolas se denomina octal, y comúnmente se le conoce como "pulpo", por su aspecto.



7.8 Configuración de la gestión de una red con Packet Tracer

En esta práctica vamos a configurar la gestión de una red sencilla usando Packet Tracer. Vamos a trabajar con la red de la siguiente imagen. Toda la configuración de direccionamiento IP y routing está preconfigurada, excepto la de las interfaces que no están conectadas y que habrá que conectar en la práctica.



Como puede verse en la figura, tenemos una red sencilla de una organización formada por una sede central y una delegación. Se ha simplificado al máximo el tamaño de la red para facilitar la configuración de la parte de gestión, y de esta forma se entienda mejor, ya que la configuración que hay que realizar en los dispositivos es muy similar. Una red más grande requeriría poco más que replicar los mismos comandos de configuración en el resto de dispositivos a gestionar. Por otro lado tenemos un módulo de gestión, también sencillo, con el que gestionaremos la red. En dicho módulo hay un servidor Radius, y un NMS, por lo que es una gestión centralizada. El NMS soportará los servicios de ntp, syslog, snmp y netflow collector. Packet Tracer tiene una funcionalidad muy limitada de estos servicios, que están implementados a modo ilustrativo. Debemos imaginarnos que el NMS implementaría aplicaciones de gestión de red más complejas que mostrarían mucha información obtenida con los servicios anteriores. Por otro lado, hay un router pequeño, un Cisco 1841, que usaremos como servidor de terminales para conectarnos a los puertos de consola de los dispositivos de red. También hay un PC y un portátil de dos administradores de red.

Los requisitos para la gestión de la red son los siguientes:

- Tal y como define la arquitectura safe, usaremos gestión fuera de banda para los dispositivos de red de la sede central y gestión en banda para los de la delegación.
- Tendremos dos conexiones de gestión remotas en cada dispositivo de la sede central: una a la consola, y otra a un puerto normal, de servicio, que estará securizado.
- Se usará un servidor de terminales para el acceso remoto a consola en la sede central.
- Se permitirá el acceso vía ssh a los equipos (usando el puerto normal).
- La autenticación será vía radius en la central y local (en el propio dispositivo) en la delegación.
- Se configurarán los servicios ntp, syslog, snmp y netflow en dispositivos de red y NMS.

- Se usará la VLAN y subred indicadas en la topología.
- Se securizará la red de gestión de manera que quede aislada de la de servicio, excepto para los servicios de gestión y el acceso ssh y por consola.

7.8.1 Conexión con módulo de gestión

En este caso los equipos que forman la red son dos routers Cisco 2911 y un switch Cisco 2960. Ninguno de ellos tienen puerto de gestión, por lo que usaremos un puerto normal que haya libre y lo dedicaremos a gestión. En el caso del switch tendrá una VLAN dedicada a gestión, la VLAN 200, por lo que estará aislado del resto. En el caso del router será necesario securizar la interfaz. Esto lo haremos en el último apartado de la práctica.

1. Conectamos el Switch 1 con puertos libres de Switch0 y Router0.
2. Creamos la VLAN 200 en Switch0 y Switch1, y asociamos los puertos de la red de gestión a dicha VLAN (en Switch1 esto significa todos los puertos con elementos en la red de gestión). Esto puede hacerse en la interfaz gráfica, o en CLI en modo configuración (el Cisco 2960 no implementa el comando 'vlan database').
3. Configuramos las IPs de los equipos de gestión para poder acceder a ellos. En el Router0 lo haremos en la interfaz que hemos conectado al módulo de gestión. En el Router1 no es necesario configurar nueva IP, ya que lo gestionaremos en banda, y usaremos la IP de una interfaz de servicio para acceder a él. En los switches crearemos una 'interface vlan 200', a la que asignaremos la IP. Como sabemos, un switch sólo trabaja a nivel 2, no mira la IP de los paquetes. Sin embargo, permite la configuración de una IP para poder acceder a él para gestionarlo, por lo que en la VLAN en que configuremos la IP, el switch procesará también la capa IP.

```
interface vlan 200
 ip address [IP] [máscara]
 no shutdown
 exit
```

4. Configuración de default gateway en switches. Al igual que en cualquier host, será necesario configurar un default gateway a donde el switch pueda enviar los paquetes que vayan a una subred distinta a la configurada. El default gateway será la IP de la interfaz del router en la subred. Se configura a nivel global en el switch.

```
ip default-gateway [IP]
```

7.8.2 Acceso ssh con autenticación Radius (central y módulo gestión)

1. Configuramos el servicio AAA (Radius) en el servidor Radius.
    - En la parte de 'Network Configuration' hay que añadir los clientes radius, es decir,

los dispositivos desde donde llegarán las peticiones de autenticación Radius. En este caso los clientes serán los routers y switches de la red de gestión y de la central. Configuramos su nombre, su IP en la subred de gestión, y una clave compartida o secret (por ejemplo, 123456).

- En la parte de 'User Setup' hay que configurar los nombres de usuario y contraseñas de los usuarios. Vamos a crear uno con las credenciales cisco / cisco para mayor sencillez.
- Finalmente, activar el servicio (Service -> ON).

En todos los dispositivos en los que se permita el acceso ssh con autenticación radius habría que seguir los pasos que se indican a continuación. Éstos serían los routers y switches del módulo de gestión y de la sede central. En esta práctica lo haremos sólo en Terminal_server, Router0 y Switch0.

2. Activamos AAA (sin ello no funcionan los comandos AAA), configuramos que la autenticación por defecto para login sea vía radius, y configuramos el servidor radius

```
aaa new-model
aaa authentication login default group radius

!En Terminal Server:
radius-server host [IP] key [key]

!En los demás dispositivos:
radius server [nombre]
 address ipv4 [IP]
 key [key]
 exit
```

Nota: Una vez hayamos hecho esto los siguientes accesos al CLI usarán autenticación radius, y habrá que utilizar el usuario y contraseña que hemos configurado en el radius (cisco / cisco).

3. Generación de par de claves RSA (privada/pública). Ssh v2 (la versión más segura) requiere un tamaño de módulo de al menos 768 bytes. Vamos a usar módulos de 1024 bytes. Para la generación de claves es necesario que el dispositivo tenga definido hostname y domain-name.

```
hostname [hostname]
ip domain-name dasr.infor.uva.es

crypto key generate rsa general-keys modulus 1024
```

4. Configuración acceso ssh. Para poder acceder remotamente a un equipo hay que habilitar algún vty (virtual terminal line). Los vtys se pueden habilitar para acceso telnet o ssh. También se pueden configurar con autenticación local, en cuyo caso los usuarios y contraseña tienen que estar en el propio equipo, o remota, en donde pueden estar en un servidor Radius o TACACS. Nosotros configuraremos que el acceso al equipo por los vtys del 0 al 15 (hay 15) sea por ssh, y la autenticación para login, la de por defecto que se haya configurado en el equipo, que hemos definido en un paso anterior que sea radius. Por último, configuramos una contraseña para el acceso a modo enable, ya que si no hay contraseña configurada, al acceder vía ssh no dejaría ponerse en modo enable. Para mayor sencillez configuraremos como contraseña: cisco

```
line vty 0 15
 login authentication default
 transport input ssh
 exec-timeout 20       !Expira sesión tras 20 minutos inactiva
(default=10)
 exit

enable password cisco
```

7.8.3 Acceso ssh con autenticación local (delegación)

En la delegación configuraremos el acceso ssh, pero en este caso con autenticación local. Por lo tanto, no será necesario activar AAA ni configurar servidor radius, y habrá que configurar usuarios y contraseñas locales. El resto de comandos de configuración son similares a los anteriores.

```
hostname [hostname]
ip domain-name dasr.infor.uva.es

crypto key generate rsa general-keys modulus 1024

line vty 0 15
 login local
 transport input ssh
 exec-timeout 20       !Expira sesión tras 20 minutos inactiva
(default=10)
 exit

username cisco password cisco
enable password cisco
```

7.8.4 Comprobación acceso ssh

Con la configuración anterior debería ser posible el acceso ssh desde los PCs a cualquier equipo de red. Para ello, en 'Desktop > Command Prompt', ejecutaremos el comando ssh, usando como *target* la IP de gestión del equipo, excepto en la delegación donde usaremos la IP de la interfaz serial. Una vez conectados al equipo con ssh, podremos desconectarnos ejecutando el comando 'exit'.

7.8.5 Acceso por consola

Conectamos el portátil de administración mediante un cable de consola al puerto de consola y/o auxiliar de alguno de los equipos (por ejemplo Router0), para simular una conexión en local, y comprender para qué sirve un puerto de consola. En el PC abrimos un terminal (Desktop > Terminal) y podemos ver cómo lo que aparece es exactamente lo mismo que se ve en el equipo en la pestaña de CLI. Si escribimos algo, lo veremos en la pestaña CLI. Tras esta comprobación, quitamos el cable de consola.

Terminal server

1. **Guardamos la configuración del terminal server, para no perderla**, e insertamos el módulo HWIC-8A en slot libre de la derecha, y conectamos con un cable octal (pulpo) los puertos Async0/0/0 y Async0/0/1 con las consolas de Router0 y Switch0. Tras esto, al ejecutar 'show line' en el terminal server veremos que aparecen las 8 nuevas líneas asíncronas.

2. Las nuevas conexiones asíncronas se corresponden en la configuración del router Terminal server con las líneas 0/0/0 a la 0/0/7. Vamos a habilitar en estas líneas lo que se denomina *telnet inverso*. Esto consiste en configurar puertos tcp de manera que al hacer telnet al terminal server a uno de esos puertos, el terminal server establecerá una conexión por el puerto serie a la consola que corresponda con el puerto. Esto se entenderá mejor cuando más adelante lo probemos. De momento, configuraremos las líneas en el terminal server, permitiendo telnet de entrada, y quitando el login para que no intente autenticar el terminal server al hacer el telnet.

```
line 0/0/0 0/0/7
 transport input telnet
 no login          !OJO esta línea se pierde al reiniciar el
router (bug) y deja de funcionar
 exit
```

3. Configuramos una interfaz de loopback, que nos permitirá lanzar un telnet desde el terminal server a sí mismo, para conectarnos a las consolas.

```
interface Loopback0
 ip address [ip_loopback0] [máscara]
```

4. (Opcional) Con el comando de configuración 'ip host' asociamos un nombre a la IP de loopback y el puerto correspondiente a cada consola. Esto hace que al ejecutar en modo enable el nombre, se lance automáticamente un telnet a la IP y puerto configurados. O lo que es lo mismo, nos podremos conectar a la consola con solo poner el nombre del dispositivo al que nos queremos conectar. Para conocer el puerto que corresponde con cada cable asíncrono, ejecutamos 'show line', y el puerto será el 20xx, donde xx es el número de línea que muestra la salida del comando. Por ejemplo, si la salida es la siguiente:

```
terminal-server#sh line
   Tty Line Typ     Tx/Rx    A Roty AccO
AccI   Uses   Noise  Overruns   Int
*    0    0
CTY              -    -    -    -      0       0     0/0       -
     1    1
AUX   9600/9600  -    -    -    -      0       0     0/0       -
 0/0/0    2
TTY   9600/9600  -    -    -    -      3       0     0/0       -
 0/0/1    3
TTY   9600/9600  -    -    -    -      0       0     0/0       -
 0/0/2    4
TTY   9600/9600  -    -    -    -      0       0     0/0       -
 0/0/3    5
TTY   9600/9600  -    -    -    -      0       0     0/0       -
 0/0/4    6
TTY   9600/9600  -    -    -    -      0       0     0/0       -
```

Los puertos tcp correspondientes a las líneas 0/0/0 y 0/0/1 serían respectivamente 2002 y 2003.

Una vez sabemos los puertos, configuramos los nombres de host, por ejemplo:

```
ip host router0 2002 [ip_loopback0]
ip host switch0 2003 [ip_loopback0]
```

En equipos reales también se podría configurar un menú, de forma que el propio menú ofreciese un listado de las consolas, pero esta funcionalidad no está implementada en Packet Tracer.

Sede central (Router0, Switch0)

Configuramos que el acceso por consola se autentique vía radius, de manera similar a como hicimos en los VTYs. En este caso no usaremos ssh, ya que necesitamos distinguir los puertos al haber usado un cable octal, y el acceso a consola será mediante telnet.

```
line con 0
 login authentication default
 exec-timeout 20       !Expira sesión tras 20 minutos inactiva
(default=10)
 exit
```

Por un bug de Packet Tracer, el Switch0 puede mostrar sólo 'login' en lugar del 'login authentication default' que hemos configurado, pero debería autenticar vía radius.

Comprobación acceso remoto por consola

Podemos conectarnos a las consolas de Router0 y Switch0 desde el propio terminal server, o desde un PC. El proceso de conexión es similar, pero el de desconexión es algo distinto:

Desde terminal server

Podemos usar el comando 'telnet [*ip*] [*puerto*]', siendo [*ip*] la IP de loopback que hemos configurado, y [*puerto*] 20xx, donde xx es el número de línea, como hemos visto antes. Por ejemplo:

```
#telnet [ip_loopback0] 2002
```

También podemos usar el nombre de host que hemos configurado:

```
#router0
```

Una vez estamos en la consola remota, para desconectarnos hay que seguir los siguientes pasos:

- Pulsar la combinación de teclas ctrl + shift + 6 y soltar las teclas

- Pulsar la tecla 'x'

Con ello volvemos al terminal server, pero si pulsamos intro sin ejecutar un comando, reanudamos la conexión a la consola de nuevo, con lo que **no hay que pulsar intro**. Lo que haremos es encontrar el número de sesión activa con el comando 'show sessions', y matarla con el comando 'discconect [*nº_sesión*], por ejemplo:

```
#show sessions      !Vemos las sesiones activas
#disconnect 1       !Matamos la sesión 1 (si sólo hay una será la 1)
```

Desde PC

Para conectarnos desde un PC, en 'Desktop > Command Prompt', ejecutaríamos el mismo comando telnet que hemos visto en la conexión desde el terminal server: 'telnet [*ip*] [*puerto*]'. En este caso, la [*ip*] podría ser o bien la IP de loopback del terminal server, como antes, o la IP de su interfaz, por ejemplo:

```
#telnet [ip_interfaz_terminal_server] 2002
```

Una vez estamos en la consola remota, para desconectarnos hay que seguir los siguientes pasos:

- Pulsar la combinación de teclas ctrl + 

- Tras lo anterior, nos aparecerá el prompt del PC (C:\>). Debemos escribir 'quit' y pulsar intro para salir del telnet[1]. Si pulsamos intro directamente sin escribir nada, reanudará el telnet.

7.8.6 Sincronización de reloj con NTP

NTP (Network Time Protocol) es un protocolo que permite la sincronización del reloj de sistemas informáticos conectados en red. Usa el puerto UDP 123. NTP organiza los sistemas en niveles, denominados estratos. El estrato 1 sería la fuente más fiable de reloj, normalmente un GPS o reloj atómico. Los sistemas de estrato 2 sincronizarían su reloj con los de estrato 1, los de estrato 3 con los de estrato 2, y así consecutivamente.

Un dispositivo de red generalmente usa para la hora un reloj interno por defecto. Cuando tenemos una red con muchos equipos de red, puede ser un problema que cada uno tenga una hora, por lo que es recomendable que el reloj esté sincronizado. Lo normal es formar una jerarquía, donde varios equipos se sincronizan desde un reloj externo, muy fiable, y luego vamos formando distintos estratos con el resto de dispositivos.

Al sincronizar toda una red por NTP, corremos el riesgo de que ocurra un problema en alguno o todos los equipos maestros, y se produzca una desincronización, o incluso peor, una variación brusca en el reloj. Esto puede producir en ocasiones problemas catastróficos, por ejemplo, si un equipo tiene que realizar algún cálculo con la hora, y el resultado es un valor negativo.

[1] Esta combinación de teclas no funciona en mac.

En esta práctica, realizaremos una configuración sencilla de NTP, tan solo para ver cómo se configura y cómo funciona, en la que el NMS será el reloj maestro (esto no sería así en la realidad), y el resto de equipos de la red sincronizan su hora con la suya. Los pasos a seguir serían los siguientes:

1. Configuramos la hora en servicio NTP en el NMS y activamos servicio si no lo está ya.

2. Configuramos en los dispositivos de red la sincronización de la hora vía ntp. Es recomendable ejecutar antes y después el comando 'show clock detail' para ver el cambio.

```
ntp server [ip]          ! Sincroniza reloj software vía ntp
ntp update-calendar      ! Sincroniza reloj hardware vía ntp.
Sólo en router
```

3. Comprobamos el funcionamiento (puede tardar varios segundos desde que se configura NTP hasta que la hora está sincronizada por NTP).

```
#show clock detail
#show ntp status
#show ntp associations
```

7.8.7 Configuración de syslog

Syslog es un estándar que especifica un formato de mensajes de log de sistemas informáticos, y un protocolo para transmitir dichos mensajes entre sistemas informáticos. Usa el puerto UDP 514. En una red, el syslog se usa para generar registros de eventos significativos. Estos registros pueden enviarse a un NMS, que los procese y almacene, generando estadísticas, gráficas, alarmas, etc. Es bastante útil en la gestión de fallos de una red, para monitorización y troubleshooting. Los logs se clasifican en prioridades o severidades, y puede configurarse en un dispositivo que se envíen al NMS únicamente los logs de ciertas prioridades, e incluso definir filtros para restringir de forma más específica lo que se envía. En nuestro caso usaremos la configuración por defecto. Para ver la configuración actual de syslog en un equipo Cisco podemos ejecutar:

```
#show logging
```

Veremos que aparece la configuración de varios syslog:

- Syslog de consola: El que envía logs a la consola.
- Syslog monitor: El que aparece en conexiones telnet y ssh
- Syslog buffer: Define el almacenamiento en el propio dispositivo de mensajes de log
- Trap: Mensajes de syslog enviados a un servidor de syslog o NMS.

Configuraremos el syslog siguiendo los siguientes pasos.

1. Activamos el servicio syslog en el NMS (ya está por defecto)

2. Configuramos el syslog server en equipos de red.

```
#logging host [ip]
```

3. Comprobamos que los mensajes de syslog llegan al NMS (en Services > syslog). Comprobamos también la configuración en los equipos de red:

```
#show logging
```

7.8.8 Configuración de SNMP

SNMP es un protocolo de gestión de red, que permite el intercambio de información de gestión entre elementos de red (NMSs y elementos gestionados). Tiene 7 operaciones o comandos básicos (formalmente *PDU types*):

- **GetRequest**: NMS solicita información de un objeto a elemento gestionado
- **GetNextRequest**: NMS solicita información del siguiente objeto a elemento gestionado
- **GetBulkRequest**: NMS solicita información de un conjunto de objetos a elemento gestionado
- **SetRequest**: NMS envía información a elemento gestionado (normalmente para configurar un valor)
- **Response**: Respuesta a una petición, de elemento gestionado a NMS.
- **Trap**: Notificación asíncrona de evento de elemento gestionado a agente
- **InformRequest**: Típicamente notificación asíncrona con ACK, de NMS a NMS

SNMP usa el puerto UDP 162 para el envío de traps, y el 161 para todo lo demás. SNMP tiene una gran flexibilidad y múltiples usos, como es obtener la configuración de los dispositivos, su estado, estadísticas, permite configurar dispositivos desde un NMS, la generación de eventos para monitorización de alarmas con traps, etc. Debido a ello, la configuración de SNMP puede

ser muy compleja. Packet Tracer no incluye prácticamente configuración de SNMP, por lo que únicamente podremos ver a modo ilustrativo cómo desde el NMS podemos, a través de SNMP y usando algunas pequeñas MIB que implementa Packet Tracer, obtener información de routers y switches, y configurar algún parámetro en ellos.

1. En Router0 configuramos las *communities* de sólo-lectura y lectura-escritura. Las *communities* son palabras clave que se configuran en NMS y elemento gestionado, y que deben coincidir para permitir el acceso por SNMP al elemento gestionado.

```
snmp-server community dasr_ro RO
snmp-server community dasr_rw RW
```

2. En el NMS, en 'Desktop > MIB Browser', ponemos la IP de gestión del Router0, y en 'Advanced' las communities. Vemos que podemos elegir entre las 3 versiones de SNMP. Recordemos que la única que es segura es la v3. Podemos navegar en el árbol de la MIB, y elegir algún objeto del que queramos obtener información. Lo seleccionamos, elegimos la operación SNMP y pulsamos en GO.

   Podemos usar Get o Get Bulk para obtener información de sistema e interfaz. También podemos usar el Set para configurar algún valor, por ejemplo, podemos cambiar el sysName del router (eligiendo DataType= OctetString), y luego volverlo a dejar como estaba. No podemos cambiar el valor de todos los objetos, ya que la MIB define cuáles son de sólo lectura y cuáles se pueden modificar.

7.8.9 Configuración de Netflow

Netflow es un estándar para recolectar información de tráfico de red. Permite enviar información de tráfico de red (estadísticas de los distintos flujos que pasan por un puerto) a un NMS (recolector Netflow), y que así en el NMS se pueda visualizar mediante estadísticas y gráficas el tráfico de una red. Vamos a configurar una pequeña funcionalidad que implementa Packet Tracer, y que permite hacerse una idea de lo que se podría conseguir con Netflow.

1. Activamos Netflow en las interfaces de servicio de Router0.

```
interface gi0/0
 ip flow egress
 ip flow ingress
 exit

interface gi0/2
 ip flow egress
 ip flow ingress
 exit

interface se0/0/0
 ip flow egress
 ip flow ingress
 exit
```

2. Enviamos las estadísticas al NMS. El Netflow Collector de Packet Tracer escucha en el puerto UDP 9996, por lo que configuraremos éste en el router.

```
ip flow-export destination [ip] [port]
ip flow-export version 9
```

3. En el NMS, en 'Desktop > Netflow Collector', activar el servicio.

4. Comprobación del funcionamiento:

   - Desde PC0 lanzar un ping continuo hacia PC2.
   - Desde PC1, en 'Desktop > Traffic Generator', generar tráfico HTTP a servidor Web.

   Con estos flujos lanzados, en Netflow Collector veremos gráficamente los distintos fllujos que pasan por los puertos en donde hemos activado Netflow. También podemos ver la información de Netflow en Router0 con el comando:

```
#show ip cache flow
```

7.8.10 Securización de la gestión

Es necesario securizar la gestión de forma que el módulo de gestión quede aislado de la red de servicio, excepto únicamente para las comunicaciones necesarias para gestionar la red.

Siendo estrictos, deberían permitirse únicamente los puertos TCP y UDP necesarios para la gestión, y cortarse todo lo demás. En este ejemplo, seremos un poco más flexibles para no complicar excesivamente la práctica.

El módulo de gestión se conecta al resto de la red mediante una interfaz IP con el Router0, los puertos de consola, y un puerto Ethernet en el Switch0.

Desde el punto de vista de seguridad, el puerto de consola se considera seguro, ya que es una interfaz serie fuera de banda y no se puede acceder por él al módulo de gestión. En el caso del Switch0, la VLAN 200 está dedicada a gestión y el resto de VLANes son de nivel 2. Una VLAN en un switch es segura, no es posible que el tráfico que entra por una VLAN de nivel 2 pueda acceder a otra VLAN. Por lo tanto, tampoco es necesaria configuración en el Switch0. Lo que sí que es necesario proteger es el Gi0/1 del Router0, ya que este puerto conecta a nivel IP con el módulo de gestión. Lo protegeremos con ACLs. Como en este router se usa enrutamiento estático, no es necesario proteger los anuncios de routing. Si usase enrutamiento dinámico, habría que configurar como pasiva la interfaz Gi0/1, e impedir que se anunciase la subred de gestión a otros routers.

También es necesario proteger los accesos a los equipos mediante VTY (ssh), para que sólo se pueda acceder por ssh desde la subred de gestión.

Protección acceso ssh sólo desde subred de gestión

En los switches sólo hay conectividad ssh desde la VLAN de gestión, ya que en el resto de VLANes no hay configurada IP. Por ello, los switches ya están protegidos.

En los routers sin embargo, es necesaria protección, ya que sin ella cualquiera podría conectarse por ssh. Puedes probar a conectarte por ssh desde PC0, PC1 o PC2 a cualquier router y verás como el acceso está permitido. Para restringir el acceso por ssh sólo a usuarios de la subred de gestión, es necesario crear una ACL y añadirla en las líneas VTY. En las líneas VTY las ACLs extendidas no funcionan muy bien, por lo que es mejor usar una ACL estándar que filtre sólo por origen y permita sólo como origen la subred de gestión.

```
access-list 1 permit [MGMT-SUBNET_IP] [WILDCARD_MASK]

line vty 0 15
 access-class 1 in
```

Tras configurar este filtro en Router0 y Router1 podremos comprobar que ya no se permite el acceso a los routers desde PC0, PC1 o PC3, pero sí desde el PC Admin1.

Protección interfaz IP Gi0/1 de Router0 que conecta con módulo de gestión

En esta interfaz es necesario permitir las conectividades necesarias para gestionar el propio Router0 y también el Router1 en banda, y restringir el resto. Esto lo haremos mediante ACLs ingress y egress. En una configuración real sólo se permitirían específicamente los protocolos y puertos que se usan para gestión. En nuestro caso, para no complicar la configuración demasiado, vamos a hacerlo así para permitir la gestión de Router1, pero para Router0 permitiremos cualquier comunicación IP entre la subred de gestión y Router0.

```
access-list 101 permit ip host [IP_Router0] [MGMT-SUBNET_IP]
[WILDCARD_MASK]
access-list 101 permit udp host [IP_Router1] host [IP_NMS] eq
123                    !ntp
access-list 101 permit udp host [IP_Router1] host [IP_NMS] eq snmp
access-list 101 permit udp host [IP_Router1] host [IP_NMS] eq
514                    !syslog (unidirec.)
access-list 101 permit tcp host [IP_Router1] eq 22 [MGMT-SUBNET_IP]
[WILDCARD_MASK]   !ssh

access-list 102 permit ip [MGMT-SUBNET_IP] [WILDCARD_MASK] host
[IP_Router0]
access-list 102 permit udp host [IP_NMS] host [IP_Router1] eq
123                    !ntp
access-list 102 permit udp host [IP_NMS] host [IP_Router1] eq snmp
access-list 102 permit tcp [MGMT-SUBNET_IP] [WILDCARD_MASK] host
[IP_Router1] eq 22   !ssh

interface gi0/1
 ip access-group 102 in
 ip access-group 101 out
```

Tras esta configuración podemos comprobar que seguimos teniendo acceso ssh desde la red de gestión, que funcionan los servicios de gestión (ntp, snmp, syslog, netflow), y que no hay acceso desde otros nodos a elementos de la red de gestión.

7.8.11 Banner de bienvenida

Por cuestiones de seguridad, es importante que los dispositivos de red cuando se acceden remotamente muestren un mensaje inicial, o de bienvenida, que avise de que el acceso no autorizado está prohibido. Es recomendable que el mensaje que se muestra esté asesorado

por algún experto legal, y que no muestre ninguna información del sistema. En Packet Tracer hay un bug y no se muestra en el acceso por ssh.

```
banner motd Z
----------------------------------------
ATENCION, este es un sistema privado de la asignatura DASR. Queda
terminantemente prohibido cualquier acceso no autorizado, bajo
responsabilidad legal
----------------------------------------
Z
```

8. WLAN Wifi

8.1 Objetivo

El objetivo de esta práctica es conocer distintas formas de configurar una red Wifi.

8.2 Competencias

Tras la finalización de la práctica deberían haberse adquirido las siguientes competencias:

- Conocer distintas formas de diseñar una red Wifi: con autenticación en puntos de acceso, con autenticación delegada a servidor Radius, usando un controlador de acceso.
- Saber cómo configurar los distintos tipos de red Wifi anteriores con puntos de acceso, routers y controladores de acceso Cisco.

8.3 WLAN Wifi

Packet tracer incluye dispositivos que permiten implementar WLANs Wifi de distinta forma. En esta práctica veremos 3 de estas formas:

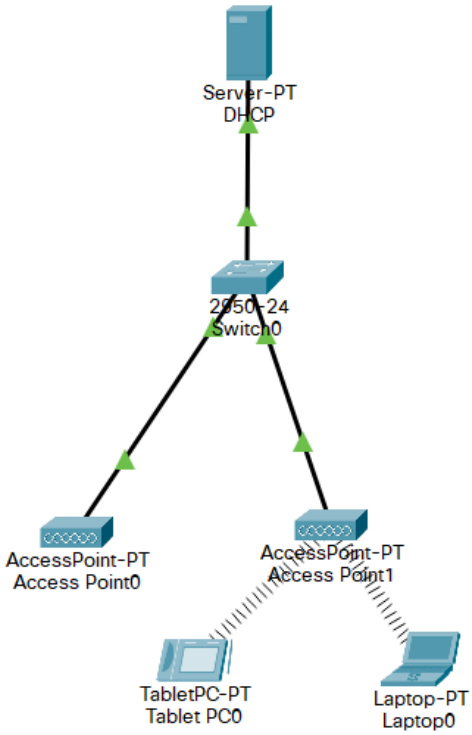
A. WLAN Wifi usando autenticación en Access Points
B. WLAN Wifi usando router Wifi y autenticación en servidor Radius
C. WLAN Wifi usando Wireless LAN Controller, Light Weight Access Points y autenticación en servidor Radius

En todas ellas necesitaremos un terminal de usuario Wifi en Packet Tracer para poder hacer pruebas. Podemos usar Tablets, Smart Phones o portátiles. En el caso de un portátil, por defecto no tiene instalada tarjeta de red Wifi. Es necesario: entrar en la configuración física; apagarlo; quitar la tarjeta de red Ethernet (arrastrándola a la parte de módulos de la izquierda); instalar una tarjeta de red Wifi (arrastrando una, por ejemplo PT-LAPTOP-NM-1W-AC, desde la parte de módulos de la izquierda hasta el slot que ha quedado libre); y encenderlo.

8.3.1 A. WLAN Wifi usando autenticación en Access Points

En este tipo de WLAN se usan puntos de acceso (AP) Wifi que no soportan autenticación delegada a un servidor Radius, y por lo tanto autentican ellos a los usuarios. Tienen un puerto Ethernet para conectarlos a una red cableada, típicamente a un Switch. Esto nos permite dedicar una o varias VLANes (en función de la topología) a la conexión Wifi. Se ubican APs donde se requiera, la autenticación se realiza mediante clave compartida, que hay que configurar en los APs, y todos los usuarios usarán la misma.

Vamos a configurar la red de la siguiente imagen.



El AP en este caso es un gateway entre la red cableada y la red Wifi, haciendo el papel de un switch que trabaja a nivel 2 (por lo que no tiene IP). Los terminales de usuario cogerán la IP del servidor DHCP. Los pasos a seguir serían los siguientes:

1. Lo único que hay que configurar en el AP es el método de autenticación, la clave compartida, y el algoritmo de encriptación. Configuraremos la más segura que permita el AP, en este caso WPA2-PSK, con clave compartida la que queramos (por ejemplo 12345678) y encriptación AES. En los puntos de acceso se puede reducir la cobertura a 40 o 50m, para que no se influyan los distintos escenarios entre sí.
2. En los terminales Wifi de usuario tendremos que configurar lo mismo en la interfaz Wireless0, y activar la configuración de la dirección IP de la interfaz y del default gateway vía DHCP. En el portátil, recuerda cambiar la tarjeta de red Ethernet por una Wifi, como se explicó más arriba.

Con ello el usuario podrá moverse, y cambiar de AP conservando la dirección IP, por lo que prácticamente no notará el cambio de AP.

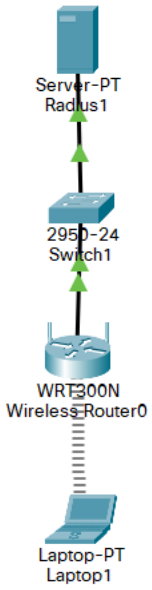
8.3.2 B. WLAN Wifi usando router Wifi y autenticación en servidor Radius

También puede usarse un router Wifi similar a los que solemos tener en casa, como el WRT300N de Packet Tracer. Este router tiene una interfaz 'Internet', con la que se conecta a la red cableada, una interfaz Wireless, y varias interfaces Ethernet etiquetadas como LAN. El router hace de switch entre la interfaz Wireless y las LAN, y de router entre todas ellas y la interfaz Internet. Estos routers permiten autenticación local (al igual que el caso anterior), pero también permiten realizar autenticación delegada a un servidor Radius remoto, de forma que

cada usuario podrá tener un nombre de usuario y contraseña. Esto es lo que vamos a configurar.

> **Nota:** Para la autenticación delegada a un radius se usa el método de autenticación WPA2-Enterprise, que a su vez usa 802.1X para permitir una autenticación delegada a un servidor. El funcionamiento de 802.1X en una red Wifi es similar al que vimos en la práctica de una red cableada, salvo que en este caso el protocolo EAP va encapsulado en Wifi (802.11) en lugar de en Ethernet.

Trabajaremos con la red de la siguiente imagen. Los pasos a seguir se indican a continuación.



1. Configura en el servidor Radius una dirección IP estática en la interfaz Fa0 (*ip_radius*). Configura también el servicio AAA (Radius). En la parte de "Network Configuration" hay que añadir los clientes Radius, es decir, los dispositivos desde donde llegarán las peticiones de autenticación Radius. En este caso el cliente será el router WRT300N. Le daremos un nombre cualquiera (es un mero ID local), una dirección IP (*ip_wrt300n0*), y una clave compartida o secret cualquiera (secret_radius). En la parte de 'User Setup' hay que configurar los nombres de usuario y contraseñas de los usuarios.
2. El router WRT200N tiene dos pestañas de configuración: Config y GUI. Configuramos primero la pestaña Config.
    a. En la interfaz 'Internet' configuramos la dirección IP que en el punto anterior definimos para el cliente radius (*ip_wrt300n0*). No vamos a usar Default Gateway, pero podemos poner una IP que daríamos a un hipotético router que estuviese conectado a nuestra red.
    b. En 'LAN' configuraremos la dirección IP del router para la WLAN formada por los puertos LAN y Wireless En un paso posterior haremos que el router sea también un servidor DHCP para los dispositivos que se conecten a él en las interfaces LAN y Wireless, por lo que esta IP deberá pertenecer a la subred que asignemos a la WLAN.
    c. En la interfaz 'Wireless' configuraremos el SSID que radiará y la autenticación. En

este caso seleccionaremos WPA2 (es decir, WPA2-Enterprise), y al hacerlo se habilitará la sección de configuración del servidor Radius, donde pondremos la IP del servidor Radius (*ip_radius*), la clave compartida entre cliente y servidor Radius (secret_radius) y el tipo de encriptación (AES).

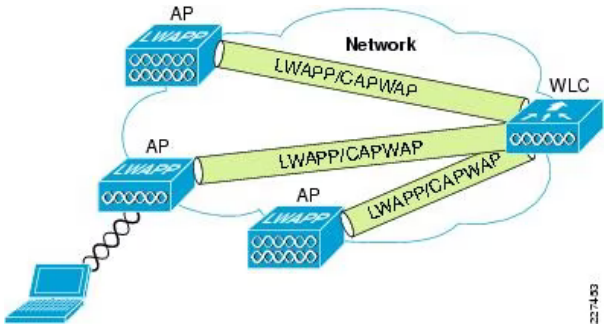
3. Realizaremos el resto de configuración del router en la pestaña GUI. Para facilitar la configuración de este modelo de router, Packet Tracer nos muestra en una nueva pestaña el GUI Web de configuración del router, al que normalmente se accedería conectándonos con un navegador Web a la IP del router (esto también podemos hacerlo, conectándonos por ejemplo desde el servidor Radius por https con el navegador Web, https://[*ip_wrt300n0*], y usando el usuario y contraseña por defecto de este router, que es admin / admin). Dentro del GUI, en la pestaña 'Setup' configuramos, si no lo está ya, la parte de 'Internet Setup' (interfaz Internet), y 'Network Setup' (interfaces LAN y Wireless). En Internet Setup al haber configurado antes la interfaz internet, debería haberse configurado la misma información (tipo de conexión estática, y las IPs que hemos configurado). En Network Setup también debería aparecer la configuración que hicimos en la pestaña LAN. Si no estuviera, configuramos y activamos el servidor DHCP y la IP del router, para que el router asigne IPs a los dispositivos que se conecten a él.
4. Añadimos en Packet Tracer uno o varios terminales de usuario inalámbricos, y configuramos su interfaz Wireless con el SSID de la red Wifi del router, autenticación WPA2, usuario y contraseña alguno de los configurados en el servidor radius, encriptación AES y configuración IP por DHCP. Con esto deberían adquirir IP y tener conectividad entre sí y con el servidor.

8.3.3 C. WLAN Wifi usando Wireless LAN Controller, Light Weight Access Points y autenticación en servidor Radius

Las anteriores formas de implementar Wifi tienen distintos inconvenientes, como son:

- Poca seguridad en el primer tipo, ya que la clave es compartida por todos los usuarios, y se configura en cada AP.
- Roaming ineficiente en el segundo tipo, ya que no está pensado para una red amplia en donde puede ser necesario cambiar de punto de acceso.
- Difícil operación y mantenimiento de la WLAN en redes grandes en ambos tipos.

Debido a ello, existe otra solución de WLAN formada por un controlador y múltiples puntos de acceso, creándose una WLAN que abarca todos los puntos de acceso, los cuales son gestionados por el controlador. Los puntos de acceso pueden delegar la autenticación del usuario en el controlador, y éste a su vez puede delegarla en un servidor Radius. La comunicación entre puntos de acceso y controlador va cifrada, utilizando los protocolos LWAPP o CAPWAP. La RFC 5416 especifica CAPWAP para redes Wifi, y denomina al controlador Access Controller (AC) y a los puntos de acceso Wireless Termination Points (WTPs). Cisco tiene su propia nomenclatura para estos dispositivos, llamando Wireless LAN Controller (WLC) al controlador, y Light Weight Access Points (LAPs) a los puntos de acceso.

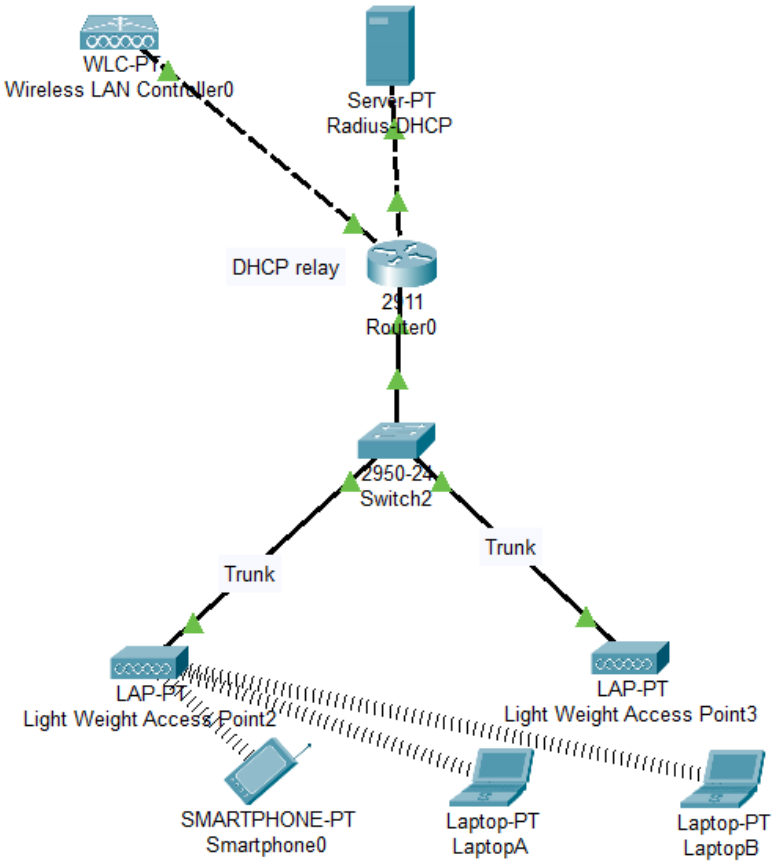


Fuente: Cisco. Small Enterprise Design Profile (SEDP)—Wireless LAN Design. *https://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Small_Enterprise_Design_Profile/chap4sba.pdf*

En los siguientes recursos puede obtenerse información detallada de CAPWAP.

- Cisco Unified Wireless Technology and Architecture
- Cisco Small Enterprise Design Profile(SEDP)—Wireless LAN Design
- ccnadesdecero - Funcionamiento CAPWAP
- RFC 5416

En esta práctica realizaremos una configuración básica en Packet Tracer de una red formada por un WLC y varios LAPs, en la que habrá dos WLANes, con SSIDs distintos, simulando, por ejemplo, una red de empleados y una de invitados. Trabajaremos con la red de la siguiente imagen. Los pasos a seguir se indican a continuación.



Nota: El modelo 3702i de LAP tiene un bug en la versión actual de packet tracer y no funciona bien, por lo que es mejor usar el LAP-PT

1. Configura en el servidor Radius-DHCP la interfaz Fa0 y el Default Gateway. Activa y configura también el servicio DHCP con 3 Pooles, asignando en todos ellos una misma IP al WLC:
   - Pool para la gestión de la red.
   - Pool para la red Wifi que irá por la VLAN [*ID_1*][1].
   - Pool para la red Wifi que irá por la VLAN [*ID_2*].
2. Configura en el servidor el servicio AAA (Radius). En la parte de 'Network Configuration' hay que añadir los clientes radius, es decir, los dispositivos desde donde llegarán las peticiones de autenticación Radius. En este caso el cliente será el WLC. Le daremos un nombre cualquiera (es un mero ID local), la IP que hemos configurado en los pooles, y una clave compartida o secret cualquiera. En la parte de 'User Setup' hay que configurar los nombres de usuario y contraseñas de los usuarios.

[1] Asignar a las VLANes los IDs numéricos que se prefiera.

3. El Router0 ya tiene configuradas las IPs en todas las interfaces y subinterfaces, y también la VLAN Id en las subinterfaces. Configura en el Router0 DHCP relay en las (sub)interfaces gi0/0, gi0/0.20 y gi0/0.30 para que se reenvíen las peticiones DHCP al servidor DHCP.
4. En el WLC, configura el direccionamiento IP en la interfaz de gestión.
5. En el WLC se pueden configurar grupos de LAPs, y también una o varias redes Wifi, y luego asociar los grupos de LAPs a las redes Wifi. En el caso de usar una única red Wifi, puede configurarse que la red Wifi irá por la VLAN 0, y en ese caso el router no usará tag de VLAN 802.1q (VLAN 0 en realidad no existe, pero el router WLC-PT usa ese ID para indicar esto). Si configuramos más de una red Wifi, podemos hacer que cada una de las WLANes use una VLAN en los LAPs. El tráfico de control del WLC y de los LAPs usará la VLAN nativa (sin tag 802.1q de VLAN), que por defecto es la VLAN 1 (en otros modelos de WLC se puede configurar por qué VLAN va el tráfico de control). En nuestro caso vamos a configurar dos redes Wifi que comparten el mismo grupo de LAPs:
    a. En Wireless LANs, configura el VLAN ID [*ID_1*] y el nombre y SSID de la red que irá por esta VLAN. En la parte de autenticación selecciona WPA2, y al hacerlo se habilitará la sección de configuración del servidor Radius, donde hay que poner la IP del servidor Radius y la clave compartida y tipo de encriptación que se configuró en el punto anterior. En 'Central Control' hay que seleccionar 'Local switching, local authentication', que significa que los LAPs realizarán conmutación de paquetes, sin necesidad de que todos los paquetes vayan al WLC, y que el control de la autenticación de usuarios lo realiza el LAP. La diferencia entre autenticación central y local es que si se usa central, WLC y LAP deben estar en el mismo dominio de broadcast. Si el WLC está en la misma VLAN que los LAP, habría que usar 'central authentication', si el WLC está fuera de la VLAN, por ejemplo en un data center, como en este caso, hay que usar 'local authentication'.
    b. Cuando se termine la configuración hay que hacer clic en 'Save' en esa pestaña, para que se guarde.
    c. A continuación pulsa en 'New' y configura la segunda WLAN, con VLAN ID [*ID_2*], nombre y SSID correspondiente. El resto de parámetros de configuración, como en la anterior WLAN. Al finalizar, pulsa en 'Save' para guardar los cambios, como antes.
6. En el WLC, en 'Config > DHCP' desactivamos, si no lo está ya, el servicio DHCP.
7. En los LAPs primero hay que ponerles la fuente de alimentación en la pestaña 'Physical', y después activar, si no lo está ya, la configuración de la IP por DHCP en Settings.
8. Añadimos en Packet Tracer uno o varios terminales de usuario inalámbricos, y configuramos la interfaz Wireless con el SSID que queramos de los dos configurados, autenticación WPA2 (es decir, WPA2-Enterprise), usuario y contraseña alguno de los configurados en el servidor radius, encriptación AES y configuración IP por DHCP. Con esto deberían adquirir IP correspondiente a la WLAN elegida y tener conectividad entre sí y con el servidor.

9. Firewalls

9.1 Objetivo

El objetivo de esta práctica es aprender las nociones básicas de funcionamiento y configuración de Firewalls en una red.

9.2 Competencias

Tras la finalización de la práctica deberían haberse adquirido las siguientes competencias:

- Conocer qué es un firewall y para qué sirve en una red.
- Conocer la diferencia entre filtrado de paquetes con estado (*stateful*) y sin estado (*stateless*).
- Configurar funcionalidades básicas de seguridad en un firewall ASA de Cisco.
- Adquirir habilidades de *troubleshooting* básico para ver el funcionamiento de un firewall poder resolver problemas sencillos que aparezcan.

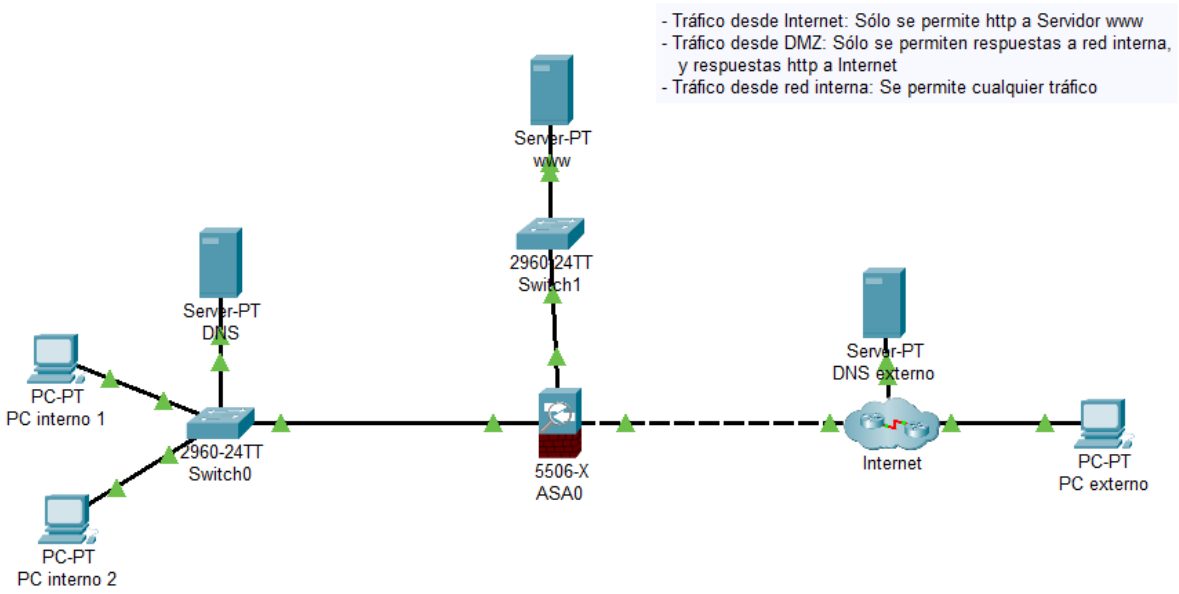
9.3 Enlaces de interés

- CCNA Security v2. Instructor Lab. Chapter 9 Lab A: Configuring ASA Basic Settings and Firewall Using CLI (web)
- CCNA Security v2. Instructor Lab. Chapter 9 Lab A: Configuring ASA Basic Settings and Firewall Using CLI (pdf)
- Cisco ASA 5506-X Configuration Tutorial – Guide

9.4 Firewalls

Un cortafuegos, o firewall, es un dispositivo o sistema, normalmente ubicado en la frontera de una red, que bloquea los accesos no autorizados a la red, mientras permite las comunicaciones autorizadas. Hay muchos proveedores y firewalls en el mercado. Algunos de los más conocidos son los ASA de Cisco, Checkpoint, Fortinet o Palo Alto. En este laboratorio vamos a realizar algunas configuraciones básicas en un Cisco ASA 5506-X que nos permitan proteger una red interna, y establecer una zona desmilitarizada (DMZ) para los servidores accesibles desde Internet. Cada modelo y proveedor de firewall utiliza comandos de configuración distintos, por lo que lo que hagamos en este laboratorio no será directamente aplicable a todos los modelos de firewalls (esto es así en cualquier equipo).

Vamos a trabajar con la red de la siguiente imagen. Toda la configuración de direccionamiento IP y routing está preconfigurada a excepción del firewall.



Como se puede ver, es una red sencilla con un pequeño campus con PCs y un servidor, y una DMZ con un servidor web expuesto a internet. El firewall ASA conecta la red con Internet. Como el objetivo de la práctica no es trabajar con NAT, en la DMZ se usa directamente direccionamiento público para mayor sencillez. Para proteger la red, es necesario realizar las configuraciones necesarias en el firewall para conseguir lo siguiente:

- Tráfico desde Internet: Sólo se permite http a Servidor www
- Tráfico desde DMZ: Sólo se permiten respuestas a red interna, y respuestas http a Internet
- Tráfico desde red interna: Se permite cualquier tráfico

El Cisco ASA no tiene contraseña de enable por defecto. Aunque al intentar entrar en el nivel privilegiado pide contraseña, no tiene, por lo que sólo habrá que pulsar intro de nuevo para entrar.

9.5 Configuración de interfaces y zonas de seguridad

En primer lugar configuraremos las interfaces del ASA. La dirección IP se configura como en cualquier router Cisco. En el caso de un ASA es obligatorio dar un nombre a cada interfaz, ya que en otros comandos de seguridad se usa el nombre de la interfaz. También es necesario asignar un nivel de seguridad a cada interfaz. El nivel de seguridad delimita zonas, ya que el ASA sólo permitirá pasar tráfico de una zona a otra zona con menor o igual nivel de seguridad. El ASA tiene predefinido que la interfaz con nombre 'inside' tiene un nivel de seguridad 100 (el máximo), y el resto de nombres 0 (el mínimo). Nosotros usaremos los nombres 'inside', 'outside' y 'dmz', y configuraremos la dmz con un nivel de seguridad 50.

```
interface GigabitEthernet1/1
 nameif inside
 ip address [ip] [máscara]

interface GigabitEthernet1/2
 nameif dmz
 security-level 50
 ip address [ip] [máscara]

interface GigabitEthernet1/3
 nameif outside
 ip address [ip] [máscara]
```

Podemos comprobar la configuración realizada con los siguientes comandos, en modo enabled, fuera del nivel de configuración:

```
ciscoasa#sh run
ciscoasa#sh interface ip brief
ciscoasa#sh ip address
```

Si una vez configurado esto realizamos pings entre los PCs internos y los PCs y servidores en la DMZ e Internet, veremos que no funciona. Si abrimos el explorador Web en un PC de la red interna e intentamos acceder a la web de la DMZ, ocurrirá lo mismo. Si realizamos alguna prueba en modo simulación veremos que en el ping el firewall descarta la respuesta (ICMP Echo reply). En http ocurre algo similar (deberemos activar http y tcp en modo simulación ya que se descarta un paquete TCP de respuesta). Como hemos dicho, por defecto el firewall no deja pasar paquetes de una zona de menor nivel de seguridad a otra con mayor nivel de seguridad.

Sin embargo, los paquetes que está descartando son paquetes de respuesta a otros que fueron iniciados desde la red interna. Esta es la diferencia entre un filtrado de paquetes con estado (*stateful*) y sin estado (*stateless*). En este caso está haciendo un filtrado sin estado, ya que no está teniendo en cuenta que el paquete de respuesta pertenece a una sesión que fue iniciada desde la zona interna. Para que realice un filtrado *stateful* debemos activar la 'inspección de paquetes' en el tráfico ICMP y HTTP. Esto se hace mediante un policy-map.

9.6 Configuración de policy-map

El comando policy-map permite aplicar políticas de seguridad. Está formado por una serie de secuencias "class", que permiten hacer match de un determinado tráfico, y aplicar una cierta acción. Una vez configurado un policy-map es necesario asociarlo con una o varias interfaces, o con todas ellas (global) para que funcione, con el comando service-policy. Esto es algo similar a las listas de acceso, que primero se definen, pero no funcionan hasta que se aplican con otro comando.

En el Cisco ASA hay preconfigurado un policy-map con nombre global_policy, aplicado a nivel global (a todas las interfaces). Este policy-map básicamente inspecciona algunos protocolos. Esto significa que el firewall será *stateful* para ellos. Lo que tenemos que hacer es añadir http e icmp a estos protocolos para que se inspeccionen también. Sin embargo, por un bug de la implementación de PacketTracer del Cisco ASA, no deja modificar el policy-map que viene por defecto, y si lo borramos y volvemos a crear, la configuración no es persistente, volverá a la inicial al reiniciar el firewall. Debido a ello vamos a crear un nuevo policy-map igual que el que hay, pero con los protocolos http e icmp. Como sólo se puede aplicar un policy-map a nivel global, aplicaremos el nuestro una a una a todas las interfaces. Posteriormente tendremos que tener cuidado si añadimos nuevas interfaces, de activar el policy-map en ellas también.

```
policy-map global_policy_dasr
 class inspection_default
  inspect http
  inspect icmp

service-policy global_policy_dasr interface inside
service-policy global_policy_dasr interface outside
service-policy global_policy_dasr interface dmz
```

Tras esta configuración si intentamos nuevamente el ping y el acceso a la web www, veremos que ya funciona, mientras que desde fuera de la red o desde la dmz no hay acceso a la red interna. Para habilitar el acceso usaremos listas de acceso.

9.7 Configuración de listas de acceso

Al igual que en los routers Cisco, los ASA también permiten configurar listas de acceso (ACL) para permitir o denegar tráfico. La configuración es las listas de acceso no es idéntica a los routers, pero es bastante parecida. La característica más diferente es que usa máscaras de subred en lugar de wildcard. Al igual que en los routers, también hay un 'deny any' implícito al final de la ACL.

Configuraremos una ACL para permitir el tráfico http de salida por la interfaz dmz.

```
access-list [nombre] extended permit tcp any host [IP_servidor] eq
www

access-group [nombre] out interface dmz
```

Una vez configurada veremos que ya funciona el acceso web desde Internet al servidor.

Como parte de los requerimientos iniciales había uno que decía que desde la DMZ sólo se podía enviar tráfico http de respuesta, pero no iniciar tráfico. Puede verse que ahora funciona el ping desde la DMZ a internet, ya que la zona dmz tiene un nivel de seguridad igual o mayor que el de internet. Para que sólo funcione el tráfico de respuesta http tendremos que añadir una ACL que deniegue el resto.

```
access-list [nombre] extended permit tcp host [IP_servidor] eq www
any

access-group [nombre] in interface dmz
```

Podemos ver las ACLs configuradas con el siguiente comando de modo enable:

```
ciscoasa#sh access-list
```

9.8 Configuración de NAT

Los Cisco ASA también permiten la configuración de NAT para traducir direcciones IP. Vamos a ver un ejemplo de configuración de PAT, ya que los comandos son algo distintos a los de los routers. En este caso, vamos a configurar PAT para que las direcciones IP privadas de la red interna se traduzcan a la dirección IP pública de la la interfaz de salida a internet del firewall en la salida a internet.

En los ASA se pueden configurar 'objetos de red' (comando 'object network'), a los que se asigna una subred, y que luego pueden referenciarse en otros comandos, como en las listas de acceso, en lugar de usar la dirección IP. La configuración de NAT se realiza en estos object network.

```
object network [nombre]
 subnet [subred_interna] [mascara]
 nat (inside,outside) dynamic interface
```

Una vez configurado, podemos comprobar su funcionamiento con los siguientes comandos 'show'.

```
sh nat
sh xlate
```

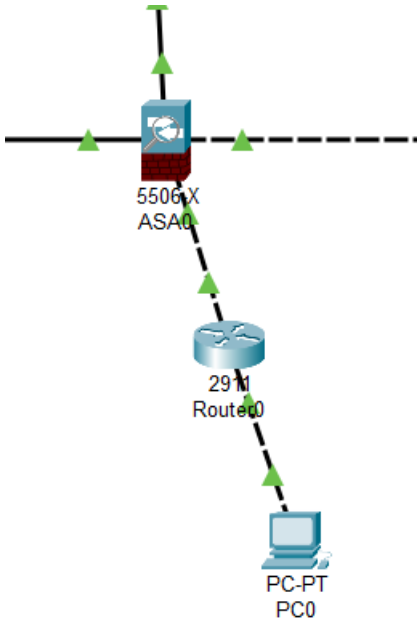
Si realizamos un ping desde un PC interno al PC externo en modo simulación, veremos que en la salida a Internet el firewall cambia la dirección IP origen, privada, por la pública de la interfaz y otro puerto.

Aunque no lo vamos a realizar, la configuración de NAT estático sería similar:

```
object network [nombre]
 host [IP_a_traducir]
 nat (dmz,outside) static [IP_traducida]
```

9.9 Enrutamiento

Los comandos de configuración y show de routing son un poco distintos en el ASA a los de los routers. Debido a ello vamos a realizar una configuración sencilla para verlos. Vamos a añadir un router y un PC a otra interfaz del firewall, tal y como se muestra en la siguiente figura. Configuramos también las direcciones IP de todas las interfaces, y del default gateway en el PC nuevo.



Mientras no asociemos la interfaz del firewall a un nivel de seguridad, y activemos el policy-map que creamos anteriormente en la nueva interfaz, el PC nuevo no tendrá conectividad con el resto de la red.

```
interface GigabitEthernet1/4
 nameif inside1
 security-level 100

service-policy global_policy_dasr interface inside1
```

Ahora nos faltaría la parte de enrutamiento para poder llegar desde la subred del PC0 al resto de redes. La configuración de routing dinámico en el ASA es prácticamente igual que en un router. Sólo hay que tener cuidado con que el ASA por defecto no envía ni acepta anuncios de routing a zonas con un nivel de seguridad inferior. Para que lo haga habría que permitirlo con ACLs.

La configuración de routing estático es algo distinta. Vamos a configurar una ruta por defecto en el router nuevo, y una ruta estática en el ASA para la red del PC0. De esta forma todas las subredes tendrán conectividad.

9.9.1 Router

```
ip route 0.0.0.0 0.0.0.0 [IP_interfaz_ASA]
```

Para ver la tabla de rutas:

```
Router#sh ip route
```

9.9.2 ASA

```
route [nameif] [subred] [máscara] [next_hop]
```

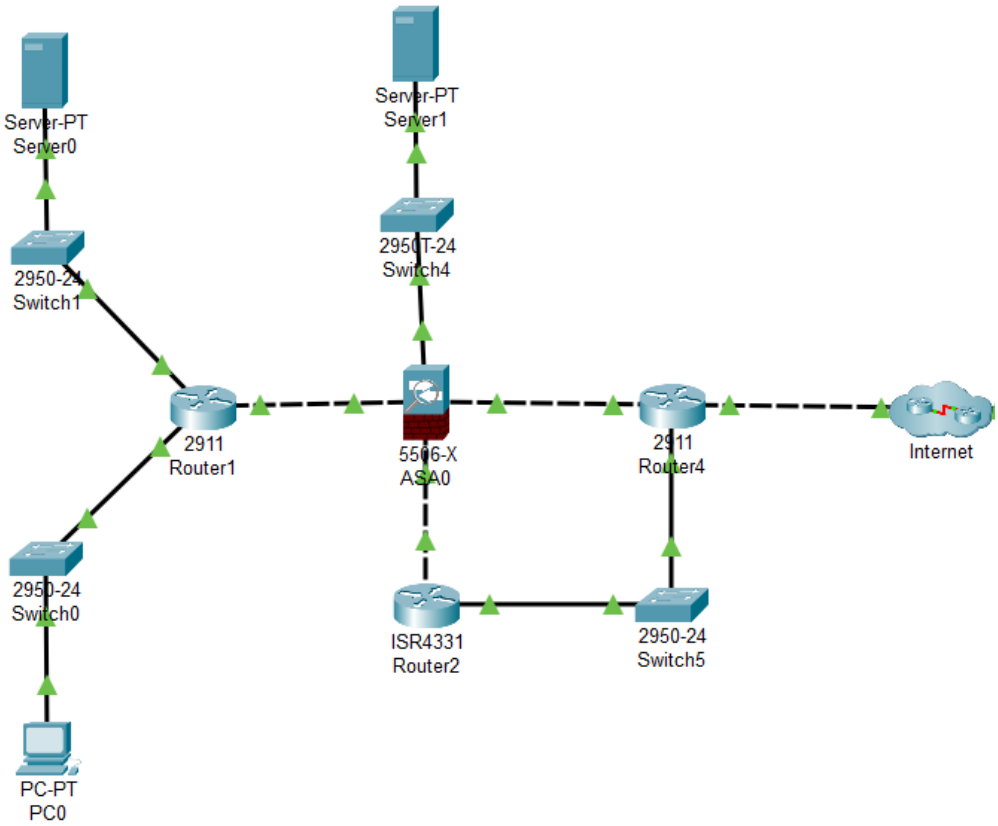
Donde [*nameif*] es el nombre de la interfaz por donde se enviará el tráfico (en nuestro caso definiremos una ruta estática para enviar el tráfico dirigido a 192.168.150.0/24 por la nueva interfaz inside1).

Para ver la tabla de rutas:

```
ciscoasa#sh route
```

9.10 Ubicación del firewall

En el ejemplo que hemos realizado el firewall es el equipo que da acceso a internet. Sin embargo, esto no tiene por qué ser necesariamente así, como hemos visto en la teoría de la asignatura. Si la red es pequeña, seguramente el equipo que da acceso a internet puede ser un firewall, o un router con ACLs. En otras ocasiones, como en redes más grandes, o por ejemplo si se quiere usar un firewall, pero éste no tiene la interfaz WAN de acceso a internet necesaria, el firewall será distinto al router de acceso a internet. En redes más grandes incluso se usarán varios firewalls. La figura siguiente muestra otro ejemplo de ubicación de firewall.


Server-PT
Server0
Server-PT
Server1
2950-24
Switch1
2950T-24
Switch4
2911
Router1
5506-X
ASA0
2911
Router4
Internet
2950-24
Switch0
ISR4331
Router2
2950-24
Switch5
PC-PT
PC0

10. VPNs

10.1 Objetivo

El objetivo de esta práctica es aprender las nociones básicas de configuración de VPNs en una red.

10.2 Competencias

Tras la finalización de la práctica deberían haberse adquirido las siguientes competencias:

- Conocer qué son y para qué sirven las VPNs site-to-site y de acceso remoto.
- Ser capaz de configurar VPNs sencillas de ambos tipos en redes Cisco.
- Entender el funcionamiento básico del establecimiento de VPN: las dos fases involucradas, qué se negocia en cada fase, y los comandos de configuración asociados.
- Adquirir habilidades de *troubleshooting* básico para ver el estado de la VPN y poder resolver problemas sencillos que aparezcan.

10.3 Enlaces de interés

- Configuración VPN site-to-site Cisco
- Cisco IPsec Troubleshooting: Understanding and Using debug Commands
- Configure Cisco Router for Remote Access IPsec VPN Connections
- Configuring RADIUS Login Authentication

10.4 Recomendaciones

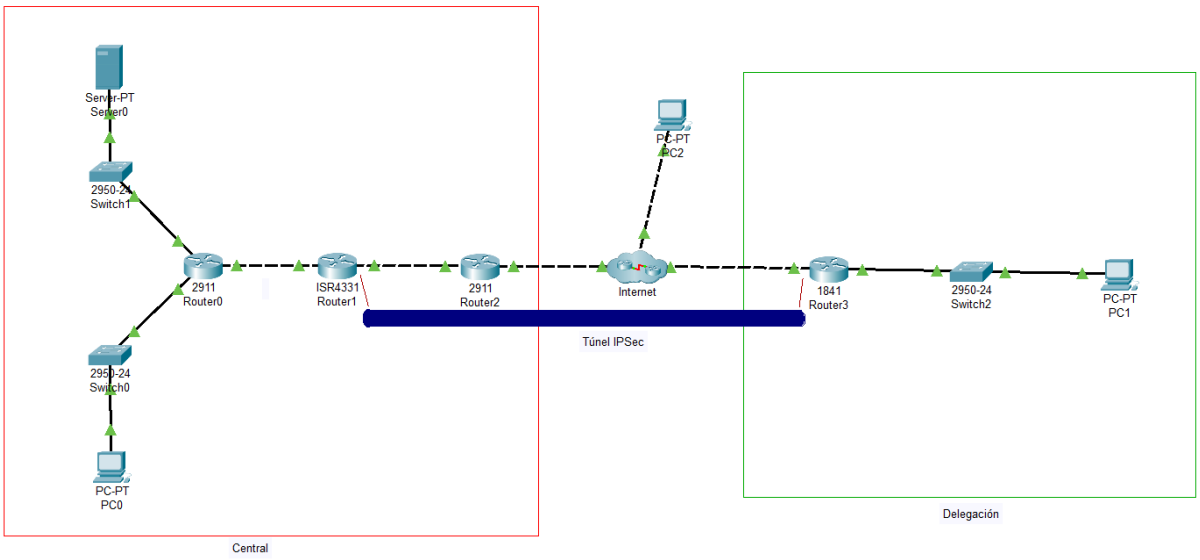
- Se recomienda que en el proyecto de laboratorio, si se requiere configurar una VPN, se usen los métodos que se explican en esta práctica, y los routers que se utilizan. IPSec es una tecnología que ya roza el límite de las capacidades de Packet Tracer, y en otros modelos de routers o firewalls de Packet Tracer puede haber bugs que hagan que algo no funcione. Por ejemplo, se ha detectado que la implementación de firewalls ASA que hay en Packet Tracer tiene bugs en alguna funcionalidad de IPSec.
- Se recomienda que en cualquier configuración de VPN IPSec que se haga en Packet Tracer, se use direccionamiento público en la interfaz donde termina el túnel IPSec. Se ha comprobado que el NAT no funciona bien con tráfico IPSec, por lo que conviene no hacer NAT sobre este tráfico (lo cual se soluciona usando direccionamiento público).

10.5 VPN sitio-a-sitio (site-to-site)

Las VPNs sitio-a-sitio sirven para conectar de forma segura oficinas dispersas geográficamente, organizaciones, delegaciones, etc. Pueden ser VPNs gestionadas por el proveedor de servicio, en cuyo caso las VPNs se terminan en un dispositivo del proveedor, o gestionadas por la propia organizador, terminándose en este caso en un dispositivo de la propia organización. Dicho dispositivo recibe diversos nombres: concentrador, terminador, cifrador, headend, etc.

Normalmente, en una VPN site-to-site se desea que cualquiera de los dos extremos pueda iniciar la conexión VPN. Es por ello que no suele usarse SSL/TLS (donde por norma general sólo uno de los extremos puede iniciar la conexión). La tecnología más común para las VPNs site-to-site gestionadas por la propia organización es IPSec. Hay distintas alternativas para configurar una VPN site-to-site IPSec. Las más comunes son mediante un túnel IPSec, un túnel GRE sobre IPSec, o un túnel virtual VTI (funcionalidad de Cisco). Como en esta práctica utilizaremos Packet Tracer, vamos a seguir el método de IPSec mediante crypto maps, que funciona bien en Packet Tracer y es relativamente sencillo. Los otros métodos o no funcionan, o dan problemas, o son demasiado complejos.

Vamos a trabajar con la red de la siguiente imagen. Toda la configuración de direccionamiento IP y routing está preconfigurada.



La red consta de una sede central y una delegación. Ambas están conectadas a internet, pero no tienen conectividad entre sí. Para conseguir dicha conectividad configuraremos una VPN IPSec a través de internet entre Router1 y Router3.

Como se puede observar, la interfaz Gi0/0/1 de Router1 tiene direccionamiento público. Esto

es así para evitar que se requiera hacer NAT del tráfico cifrado de la VPN, ya que se ha comprobado que en Packet Tracer el NAT de tráfico IPSec no funciona bien.

IPSec usa el protocolo IKE para el intercambio de claves necesario para obtener un secreto compartido en la sesión. La negociación de IKE consta de dos fases

- **Fase 1**: Se establece un canal seguro mediante ISAKMP en el que se intercambian las claves necesarias para poder crear asociaciones de seguridad (SA). Una asociación de seguridad es un canal seguro entre dos extremos, que usan un conjunto de parámetros, protocolos y algoritmos de seguridad comunes.
- **Fase 2**: Se crean SAs IPSec para los datos de los usuarios.

En los comandos de configuración y troubleshooting de Cisco se distinguen ambas fases porque en ellas se suele hacer referencia a ISAKMP (fase 1) o IPSec (fase 2).

A la hora de configurar un túnel IPSec entre dos dispositivos, es muy importante acordar los parámetros que se configurarán (protocolos, algoritmos, timers, tráfico que se permite). Estos deben ser coherentes en ambos lados del túnel, o el túnel no funcionará. Es muy común que un túnel IPSec no levante porque en ambos extremos haya algún error de configuración y los parámetros no sean iguales. IPSec es muy sensible a esto, y la negociación fallará ante cualquier pequeña variación en la configuración. Debido a ello, se recomienda que antes de configurar un IPSec se rellene un formulario como el de la siguiente tabla, y posteriormente se compruebe bien que se ha configurado lo que aparece en el formulario.

El siguiente formulario indica la configuración que realizaremos en nuestra VPN. Packet Tracer tiene implementadas versiones antiguas de protocolos de autenticación y algoritmos de cifrado. En una configuración real, se recomienda que se revise la política o procedimientos de seguridad de la empresa que contendrá recomendaciones de protocolos y algoritmos de seguridad a usar. En caso de duda, pueden consultarse las recomendaciones de organismos oficiales de seguridad, como el Centro Criptológico Nacional.

DESCRIPCIÓN	VALOR
TIPO DE VPN	IPSec con crypto-maps
IP PUBLICA ROUTER LOCAL	x.x.x.x
IP PUBLICA ROUTER REMOTO	x.x.x.x
FASE 1: ISAKMP	Autenticación: Pre-share Clave PSK: 123456 Encriptación: AES 256 Hash: SHA

	Grupo DH: 5 Lifetime: 3600
Fase 2: IPSEC	Modo: ESP Tunnel Encriptación: AES 256 Hasing: HMAC-SHA Lifetime: Default (4608000 kilobytes/3600 seconds) PFS: NO
SUBREDES LOCALES	x.x.x.x /x
SUBREDES REMOTAS	x.x.x.x /x
REGLAS NAT	No hay

10.5.1 Configuración Router1

1. Configuración de parámetros de fase 1. Se realiza mediante:

   - Un comando 'crypto isakmp policy', en donde se definen los parámetros de autenticación que se usarán. Se pueden añadir varias políticas, usando distintos índices numéricos en el comando. En la negociación, el router las recorrerá hasta que encuentre una compatible con el otro extremo.
   - Un comando 'crypto isakmp key', en el caso de usar clave compartida como tipo de autenticación, indicando la dirección IP del otro extremo del túnel y la clave compartida (en este caso 123456).

```
crypto isakmp policy 10
 encryption aes 256          !algoritmo de cifrado
 authentication pre-share    !tipo de autenticación
 group 5                     !Grupo Diffie-Hellman
 lifetime 3600               !Tiempo de vida de la SA de fase 1

crypto isakmp key 123456 address [ip_publica_router3]
```

2. Configuración de parámetros de fase 2. Se realiza mediante:

   - Un comando 'crypto ipsec transform-set', en el que se indican los protocolos y algoritmos de seguridad usados. Cisco llama "transform set" a un conjunto de protocolos y algoritmos a usar.
   - Un 'crypto map', en donde se asocia el transform-set con uno o varios destinos. El crypto map se asociará posteriormente a una interfaz, desde donde se establecerá el túnel, y sólo se puede asociar un crypto map a una interfaz. Por lo tanto, se tiene que usar un mismo crypto map para todos los túneles que terminen en una

interfaz. Cada uno de ellos usará un índice numérico en el crypto map.

- En el crypto map también se indica ('comando match address') la ACL que detectará el tráfico a cifrar. Cisco denomina "tráfico interesante" el tráfico a cifrar.
- Una ACL que se usará para definir el "tráfico interesante" que se cifrará en un túnel. Esta ACL no hace que el router descarte tráfico, sólo especifica qué tráfico se cifra. El tráfico que no permita la ACL no se cifrará (no entrará en el túnel). En la ACL se indicarán las redes origen y destino del tráfico que se cifrará. Sólo hace falta indicar el tráfico en el sentido de cifrado. No es necesario indicar el tráfico en el sentido de descifrado. Al igual que el resto de parámetros de fase 1 y fase 2, es imprescindible que el "tráfico interesante" sea el mismo en ambos extremos del túnel. En caso contrario la fase 2 no levantará.

```
crypto ipsec transform-set TS_AES_SHA esp-aes 256 esp-sha-hmac

crypto map VPN 10 ipsec-isakmp
 set peer [ip_publica_router3]
 set transform-set TS_AES_SHA
 match address 100

access-list 100 permit ip [x.x.x.x] 0.0.255.255 [x.x.x.x]
0.0.0.255
```

3. Asociación del 'crypto map' a la interfaz Física. Esto se hace a nivel de configuración de la interfaz, con el comando 'crypto map'. Una vez asociado un crypto map a la interfaz, y levantadas fase 1 y 2, el router cifrará y enviará por el túnel el tráfico interesante que salga por la interfaz.

```
interface GigabitEthernet0/0/1
 crypto map VPN
```

4. Enrutamiento de tráfico a redes remotas hacia concentrador.

   Para enviar tráfico por el túnel es necesario que previamente el tráfico esté enrutado hacia la interfaz. Esto no es tan obvio como parece, ya que las redes del extremo remoto a las que se quiere llegar por el túnel no estarán configuradas a priori en la red local. Si la interfaz del túnel es una por la que pasa todo el tráfico que sale hacia internet, no será necesario configurar nada, ya que habrá una ruta por defecto, que dirija el tráfico hacia la interfaz donde se inicia el túnel. Pero si se ubica el cifrador de otra forma, por ejemplo en una DMZ o en paralelo con un firewall, es muy probable que sea necesario añadir enrutamiento para dirigir el tráfico a las redes remotas al concentrador.
   En este caso no es necesario configurar nada.

10.5.2 Configuración Router3

La configuración del Router3 es similar a la ya descrita:

1. Configuración de parámetros de fase 1.

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600

crypto isakmp key 123456 address [ip_publica_router1]
```

2. Configuración de parámetros de fase 2.

```
crypto ipsec transform-set TS_AES_SHA esp-aes 256 esp-sha-hmac

crypto map central 10 ipsec-isakmp
 set peer [ip_publica_router1]
 set transform-set TS_AES_SHA
 match address 100

access-list 100 permit ip [x.x.x.x] 0.0.0.255 [x.x.x.x]
0.0.255.255
```

3. Asociación del 'crypto map' a la interfaz Física.

```
interface FastEthernet0/0
 crypto map central
```

4. Enrutamiento de tráfico a redes remotas hacia concentrador. En este caso no es necesario configurar nada.

5. Permitir en listas de acceso y firewalls de la red el tráfico necesario. En caso de que el concentrador se encuentre detrás de un firewall, o de un router con listas de acceso restringiendo el tráfico, es necesario permitir, por un lado, el tráfico cifrado entre internet y la interfaz que termina túnel, y por otro lado, el tráfico, una vez descifrado, entre el concentrador y el resto de la red.

   En este caso no es necesario configurar nada, ya que no hay firewall ni listas de acceso que rechacen tráfico. A continuación se indican los protocolos y puertos que usa IPSec, por si fuese necesario abrirlos en algún firewall o ACL.

Servicio	Protocol number	Puerto origen	Puerto destino
ISAKMP/IPSec Key Management	17 (UDP)	500	500
IPSec Tunnel Encapsulation	50 (ESP)	N/A	N/A
ISAKMP NAT-Traversal	17 (UDP)	4500	4500
IPSec Over UDP	17 (UDP)	10000 (default)	10000 (default)
IPSec Over TDP	6 (TCP)	10000 (default)	10000 (default)

6. En el caso de que haya NAT configurado en el concentrador, asegurarse de que el tráfico interesante entre por el túnel. Si hace NAT antes de encriptar el tráfico, puede que ya no cumpla la ACL que define el tráfico interesante que se encriptará, y no entrará por el túnel. En nuestro ejemplo, hay PAT configurado y ocurre esto. En este caso el efecto será que levantan las fases 1 y 2, pero no hay conectividad, ya que Router3 hace PAT y envía el tráfico por la interfaz, sin encriptar, con IP destino la IP privada del destino, por lo que el router de Internet lo descartará (esto puede verse haciendo ping en modo simulación).

   Lo que hay que hacer es excluir el tráfico interesante del tráfico del que se hace PAT, añadiendo para ello una entrada en la ACL 101 que deniegue explícitamente el tráfico interesante. Esta ACL se usa sólo para decidir de qué tráfico se hace NAT, no implica que al denegar un paquete éste se descarte.

```
no access-list 101
access-list 101 deny ip [x.x.x.x] 0.0.0.255 [x.x.x.x]
0.0.255.255
access-list 101 permit ip [x.x.x.x] 0.0.0.255 any
```

10.5.3 Comprobación del funcionamiento

El túnel IPSec no levantará hasta que no haya tráfico interesante que se envíe/reciba. Por lo que para que levante hay que hacer ping, por ejemplo entre el PC0 y el PC1. Los paquetes del ping se descartarán mientras el túnel esté negociando. En el mundo real, la negociación tarda poco (segundos o como mucho algún minuto), pero en Packet Tracer tarda bastante, unos 15 minutos del tiempo que marca Packet Tracer. Por lo que es conveniente dar al botón de "Fast Forward Time" hasta que pasen los 15 minutos, y volver a reintentar el ping.

Los principales comandos de *troubleshooting* para ver el estado del túnel son los siguientes:

```
show crypto isakmp sa     !Muestra el estado de la fase 1 de los
túneles
show crypto ipsec sa      !Muestra el estado de la fase 2 de los
túneles

debug crypto isakmp       !Activa el debug de fase 1
debug crypto ipsec        !Activa el debug de fase 2
undebug all               !Desactiva todos los debugs
```

10.6 VPNs de acceso remoto

Las VPNs de acceso remoto sirven para conectar usuarios específicos remotos (empleados teletrabajadores, partners) a la red corporativa. El túnel suele iniciarse en el dispositivo del usuario (ordenador, teléfono, etc). Estas VPNs usan generalmente IPSec o SSL (TLS). Si se usa IPSec, es necesario instalar un cliente en el dispositivo del usuario, debido a la complejidad de IPSec. Si se usa SSL, puede instalarse también un cliente, pero SSL permite además varias opciones de funcionamiento, que van desde no usar cliente alguno (la conexión iría desde el propio navegador de internet, si éste soporta SSL), hasta ejecutar un cliente SSL ligero o pesado desde el navegador. En esta práctica vamos a ver un ejemplo con IPSec, y otro SSL sin cliente.

10.6.1 VPN de acceso remoto IPSec

En este caso vamos a usar como terminador para la VPN de acceso remoto el mismo concentrador que en la práctica anterior, Router1: Podremos probar la VPN con un cliente VPN en el PC2 (Packet Tracer tiene incluido uno en la pestaña Desktop). Para la autenticación del usuario Cisco permite varias opciones. La más sencilla es que sea una autenticación local en el propio router, donde se configurarían usuarios y contraseñas. Otra, algo más compleja, pero más segura en redes de tamaño medio o grande, es que Router1 delegue la autenticación en un servidor Radius. Nosotros utilizaremos éste método, usando Server0 como servidor Radius.

También hay distintas opciones para la asignación de direcciones IP a los clientes VPN. En nuestro caso configuraremos el rango de direcciones IP posibles en el propio concentrador. Los pasos a seguir son los siguientes. Alguno es idéntico a la práctica anterior, y no es necesario realizarlo si ya está configurado, pero se incluye por completitud.

Configuración Router1

1. Autenticación de usuario vía Radius. Se realiza mediante:
    - El comando 'aaa new-model' que activa AAA.
    - El comando 'radius server', que configura un servidor Radius.
    - Los comandos 'aaa authentication' y 'aaa authorization', que hacen que los grupos de usuarios identificados con una etiqueta realicen su autenticación y autorización vía Radius.

```
aaa new-model

radius server radius1
 address ipv4 [x.x.x.x] auth-port 1645
 key 123456

aaa authentication login RTR-REMOTE group radius
aaa authorization network RTR-REMOTE-GROUP group radius
```

2. Configuración de parámetros de fase 1. Se realiza mediante:
    - El mismo comando 'crypto isakmp policy' ya descrito en el ejemplo anterior.
    - El comando 'ip local pool', donde se indica el rango de direccionamiento IP local que se asignará a los clientes. En este caso, la subred x.x.x.x/24
    - El comando 'crypto isakmp client configuration group' que asocia la VPN con la clave compartida (en este caso psk12345') y el direccionamiento IP.

```
crypto isakmp policy 10     !No necesario si ya está configurado
 encryption aes 256
 authentication pre-share
 group 5
 lifetime 3600

ip local pool DYNPOOL [x.x.x.x] [x.x.x.x]

crypto isakmp client configuration group RTR-REMOTE-GROUP
 key psk12345
 pool DYNPOOL
```

3. Configuración de parámetros de fase 2. Se realiza mediante:

   - El mismo comando 'crypto ipsec transform-set' que en el ejemplo anterior.
   - Un 'crypto dynamic-map', al que se asocia el transform-set, y al que se le indica que genere en la tabla de rutas una ruta hacia la subred remota.
   - Un 'crypto map'. En este caso, como a una interfaz sólo se le puede asociar un crypto map, si ya hay un crypto map configurado y asociado a la interfaz, debemos usar el mismo. Requiere varios comandos para autenticación, autorización y configuración del túnel, y luego la asociación al dynamic-map, añadiendo una nueva entrada al crypto map con un índice numérico distinto (por ejemplo el 20). Importante: Packet Tracer tiene un bug en este comando, y sólo deja meter el comando 'crypto map [*tag*] [*index*] ipsec-isakmp dynamic [*tag*]' si el crypto map ya está creado anteriormente. Si no está creado da error. En esta práctica debería ya estar creado para la VPN site-to-site, pero si no lo estuviese, habría que crearlo antes, con otro índice (aunque no usemos ese otro índice).

```
crypto ipsec transform-set TS_AES_SHA esp-aes 256 esp-sha-hmac

crypto dynamic-map DYNMAP 10
 set transform-set TS_AES_SHA
 reverse-route

crypto map VPN 10 ipsec-isakmp     !Comando para evitar bug. En
caso de que ya esté configurado, no hace falta.

crypto map VPN client authentication list RTR-REMOTE
crypto map VPN isakmp authorization list RTR-REMOTE-GROUP
crypto map VPN client configuration address respond
crypto map VPN 20 ipsec-isakmp dynamic DYNMAP
```

4. Asociación del 'crypto map' a la interfaz Física. Igual que en el ejemplo anterior.

```
interface GigabitEthernet0/0/1
 crypto map VPN
```

5. Enrutamiento de tráfico a clientes remotos hacia concentrador.

   Igual que en el ejemplo anterior, para enviar el tráfico hacia los clientes remotos por el túnel es necesario que previamente el tráfico esté enrutado hacia la interfaz. En nuestro caso, el tráfico hacia la subred x.x.x.x/24.
   En este caso, como el concentrador está en el camino de la ruta por defecto de la red, no es necesario configurar nada.

Configuración servidor Radius Server0

La configuración del servidor se hace en la pestaña 'Services'. Hay que activar el servicio AAA, dar un nombre al cliente Radius, que es el dispositivo que envía las peticiones Radius, en nuestro caso el concentrador, indicar su dirección IP, la clave compartida que hemos configurado en el concentrador, y el puerto UDP a utilizar. Toda esta información debe ser coherente con la configurada en el concentrador en la parte de Radius. Una vez escrita la configuración hay que hacer clic en el botón 'Add'.

```
Service: On
Radius Port 1645
Client Name: Router2
Client IP: [x.x.x.x]
ServerType: Radius
Key: 123456
```

También hay que dar de alta los usuarios y contraseñas que creamos convenientes en la parte de 'User Setup'.

Comprobación del funcionamiento

En este caso, primero podemos comprobar que si hacemos ping desde el PC2, situado en internet, a los equipos internos de la red, no hay conectividad. Después, usamos el cliente VPN del PC en la pestaña 'Desktop'. Hay que poner la información que hemos configurado y conectar.

```
GroupName: RTR-REMOTE-GROUP
Group Key: psk12345
Host IP (Server IP): [x.x.x.x]
Username/password: El que se haya configurado en el servidor Radius.
```

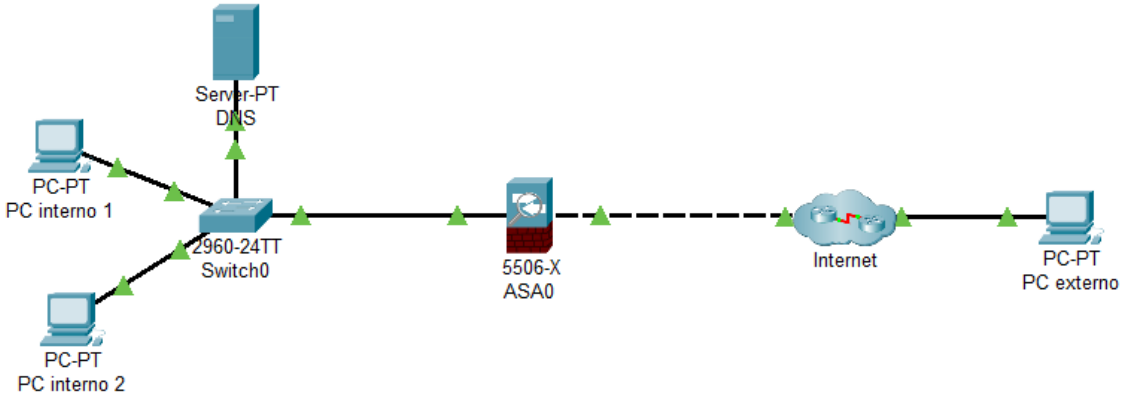
La primera vez puede tardar o fallar, se recomienda reintentar si la primera vez falla. Una vez se ha conectado, indicará la dirección IP. También puede abrirse un 'command prompt' y ejecutar 'ipconfig' en el PC, y se verá una 'Tunnel Interface', con la dirección IP asignada en el túnel. Si hacemos ping a los equipos internos de la red (por ejemplo al PC o al servidor), éste ya funcionará.

Los principales comandos de *troubleshooting* para ver el estado del túnel en el concentrador son los mismos que en el ejemplo anterior:

```
show crypto isakmp sa     !Muestra el estado de la fase 1 de los
túneles
show crypto ipsec sa      !Muestra el estado de la fase 2 de los
túneles

debug crypto isakmp       !Activa el debug de fase 1
debug crypto ipsec        !Activa el debug de fase 2
undebug all               !Desactiva todos los debugs
```

10.6.2 VPN de acceso remoto SSL *clientless*

Para configurar una VPN SSL sin cliente (*clientless*) vamos a usar un firewall Cisco ASA, que en Packet Tracer tiene esta funcionalidad. Para ello vamos a usar otra red distinta que las de los anteriores ejercicios de este laboratorio, con un firewall ASA. La red corresponde con la siguiente imagen.



En este caso, el firewall ASA incluye una funcionalidad, webvpn, que permite configurar de manera sencilla un servidor SSL, en el que configuraremos las webs internas a las que los usuarios que se conecten a la VPN podrán acceder. El usuario se conectará usando https al firewall, y éste, tras autenticarle, le presentará una web de bienvenida de la VPN, desde que podrá acceder a la web interna configurada para este usuario. En la implementación de Packet Tracer de webvpn se puede asociar a un usuario una sola web.
Este tipo de VPN es útil, por ejemplo, para dar acceso a empleados o partners a una web privada (intranet). Para este ejemplo usaremos autenticación local en el firewall ASA, configurando usuarios y contraseñas en el mismo firewall. El Cisco ASA pide contraseña para entrar a modo enable, pero no tiene puesta ninguna, sólo es necesario pulsar intro.

Los pasos a seguir son los siguientes.

1. Configurar, vía CLI en modo configuración, los usuarios en el firewall ASA.

```
username [username] password [password]
```

2. Activar, vía CLI en modo configuración, 'webvpn' en la interfaz 'outside'.

```
webvpn
 enable outside
```

3. En la interfaz gráfica del ASA, pestaña 'Config', en 'Clientless vpn > Bookmark manager', configurar la URL a la que se permite acceso desde la VPN (http://[*ip_servidor*]). Hay que dar un nombre que no contenga espacios a la URL.

4. En la interfaz gráfica del ASA, pestaña 'Config', en 'Clientless vpn > User manager', asociar el usuario al bookmark y definir un profile y group. Hacer clic en 'set'

5. Permitir que desde fuera de la red se llegue a la interfaz de FW.

6. En el PC externo, en 'Desktop > Web Browser', acceder a https://[*ip_publica_ASA*] (es https, ojo).

11. Cisco Etherchannel

11.1 Objetivo

El objetivo de esta práctica es conocer la funcionalidad de Cisco Etherchannel, que permite agregar varios enlaces Ethernet.

11.2 Competencias

Tras la finalización de la práctica deberían haberse adquirido las siguientes competencias:

- Saber en qué consiste la agregación de canales Ethernet, y cómo la implementan los routers y switches Cisco.
- Saber cómo configurar agregación de interfaces ethernet en routers y switches Cisco.

11.3 Cisco Etherchannel

Cisco permite agregar varias interfaces físicas en una única interfaz lógica a nivel 2. La interfaz lógica funcionará como una única interfaz, con el ancho de banda agregado de todas las interfaces físicas que la componen. Cisco denomina a esta interfaz lógica Etherchannel. Para negociar la agregación de enlaces entre dos dispositivos, Cisco soporta los protocolos LACP (estándar) y PAgP (propietario).

Un Etherchannel puede configurarse tanto en puertos de nivel 2 como en puertos de nivel 3. Para que un Etherchannel levante cuando se configura es necesario que:

- Todos los puertos en ambos extremos tengan la misma configuración de velocidad y duplex.
- Todos los puertos estén en estado no shutdown.
- Si es una interfaz de nivel 2, todos los puertos tengan la misma configuración de switchport (ya sea acceso o trunk).

Para agregar las interfaces se utiliza el comando a nivel de interfaz 'channel-group [*id*] mode [*modo de negociación*]'. El id tiene que ser el mismo en las distintas interfaces de un dispositivo, pero no tiene por qué ser el mismo en distintos dispositivos, ya que tiene un significado local. Los modos de negociación pueden ser los siguientes:

Modo	Protocolo de negociación	Explicación
encendido	Ninguno	Habilita EtherChannel incondicionalmente. Se recomienda si la estación de trabajo/servidor no admite ningún protocolo de negociación.
desactivado	Ninguno	EtherChannel deshabilitado incondicionalmente.
activo	LACP	Inicia la negociación enviando paquetes LACP. Se recomienda si la estación de trabajo/servidor admite LACP.
pasivo	LACP	Si el extremo remoto envía paquetes LACP, la negociación comenzará.
deseable	PAgP	Inicia la negociación enviando paquetes PAgP. Se recomienda si la estación de trabajo/servidor admite PAgP.
Auto	PAgP	Si el extremo remoto envía paquetes PAgP, la negociación comenzará.

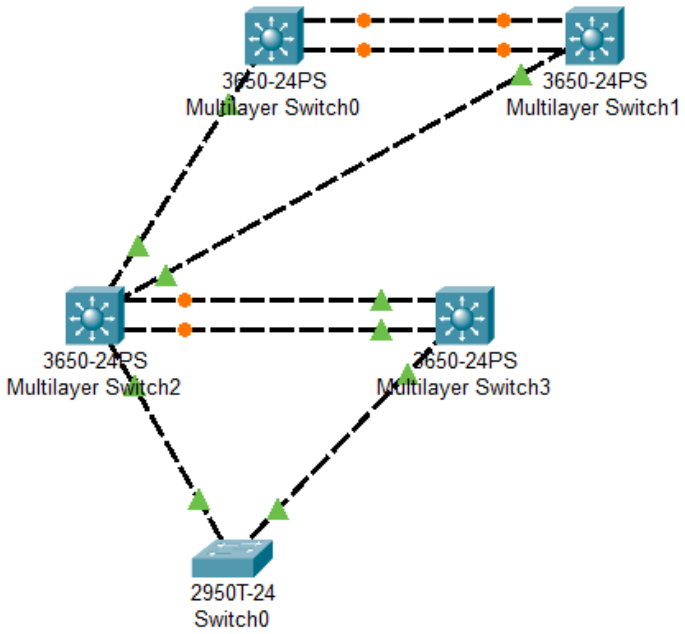
Fuente: Cisco.com https://www.cisco.com/c/es_mx/support/docs/lan-switching/etherchannel/98469-ios-etherchannel.html

En esta práctica vamos a usar mode 'active', que hace que se utilice el protocolo LACP. Una vez configurado el grupo, se crea automáticamente la interfaz port-channel (Po) correspondiente.

Puede encontrarse más información sobre cómo configurar Etherchannel en Cisco en los siguientes recursos:

- freeccnastudyguide - Apartado 6-7. Etherchannel (recursos CCNA de la asignatura)
- ccnadesdecero - Configurar etherchannel
- dummies.com - Etherchannel configuration

Vamos a configurar el siguiente ejemplo, donde tendremos dos Etherchannel, uno para interfaces IP, y otro para interfaces trunk.



Los pasos para realizar la configuración son los siguientes:

1. Activar IP routing en los multilayer switches 0 y 1
2. Configurar el etherchannel entre Switch0 y Switch1 y asignarle dirección IP. Para mayor agilidad al configurar el etherchannel puede usarse el comando de configuración 'interface range [*puertos*]'

```
Switch(config)#interface range [puertos]
Switch(config-if-range)#no switchport
Switch(config-if-range)#channel-group [id] mode [modo de
negociación]
Switch(config-if-range)#exit
Switch(config)#int port-channel 1
Switch(config-if)#ip address [IP] [máscara]
```

Los siguientes son algunos comandos de show para comprobar la configuración y estado de un etherchannel que tiene configuración IP:

```
Switch# sh etherchannel ?
  load-balance  Load-balance/frame-distribution scheme among
ports in
                port-channel
  port-channel  Port-channel information
  summary       One-line summary per channel-group
  <cr>

Switch# sh int port-channel [id]
Switch#sh ip int brief
```

3. Configurar las interfaces IP que no son Etherchannel en todos los multilayer switches.
4. Configurar el etherchannel de nivel 2. No olvidar configurar en cada interfaz el tipo access/trunk.

```
Switch(config)#int range [puertos]
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#channel-group 1 mode active
```

5. Al cabo de un tiempo la interfaz port-channel [*id*] (o de manera resumida Po[*id*]) cogerá automáticamente la configuración de trunk. Los comandos para ver la configuración y el estado son los mismos que en el anterior etherchannel, a excepción del último comando, ya que en este caso es un etherchannel de nivel 2 y no tiene IP.
6. Configurar las conexiones con el Switch0 como trunk, activar VTP en el dominio dasr en el Switch0 y crear en él la VLAN 10.
7. Comprobar que hay conectividad IP entre las interfaces IP, y que Switch2 y Switch3 muestran en 'show spanning-tree vlan 10' sólo el puerto Po[*id*] y el puerto con el Switch0. Si todavía muestra los puertos físicos que componen el Etherchannel, guardar la configuración y reiniciar el Switch.