



---

# PECL5 – SEGURIDAD EN REDES IP

---

Redes de Computadores ; Grado Ingeniería Informática



18 DE ABRIL DE 2019

ROBERT PETRISOR X9441429K Y DAVID MÁRQUEZ 47319570Z  
Laboratorio 12 – 14 H

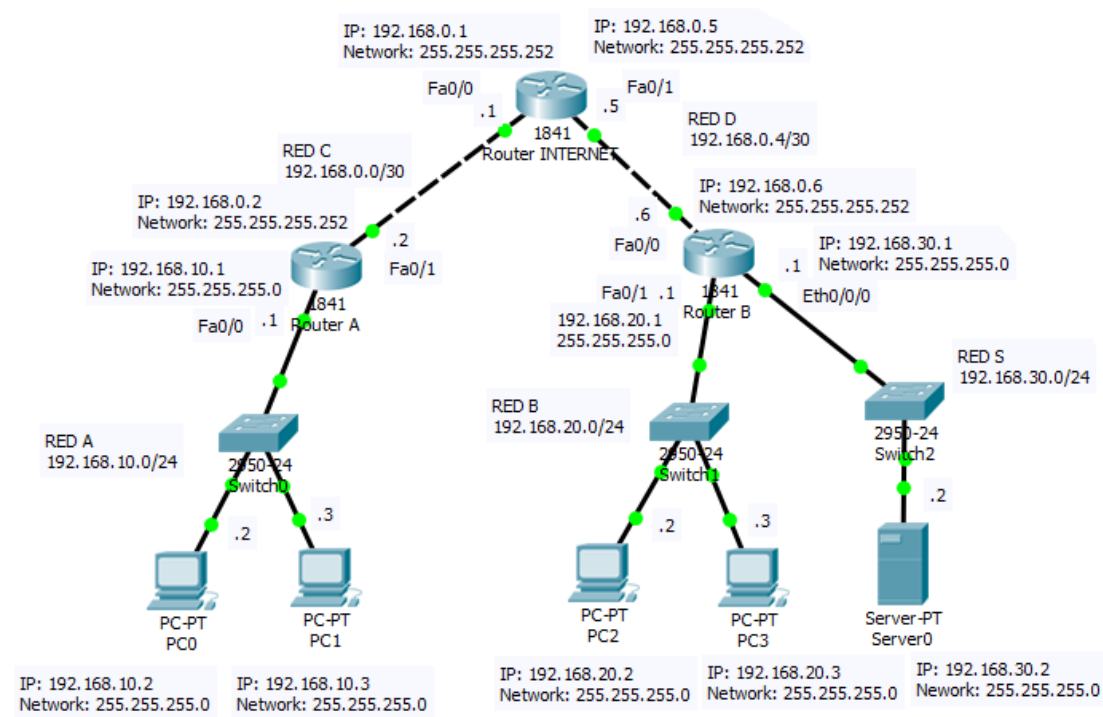
## Contenido

Ejercicio 1: Listas de acceso estándar .....	2
1.1 Crear la topología de la Red.....	2
1.2 Configuración de Interfaces, esquema de direccionamiento y tablas de enrutamiento .....	2
1.3 Verificación de la conectividad .....	4
1.4 Configuración Lista de control de acceso estándar.....	5
1.5 Comprobación de la conectividad entre todos los equipos (ping).....	6
1.6 ¿Qué cambio deberíamos de hacer en la ACL para permitir a toda y solamente a la Red A? .....	7
1.7 ¿Podemos aplicar esa ACL a otra interfaz del router B?¿Por qué o por qué no? .....	8
Ejercicio 2: LISTAS DE ACCESO EXTENDIDA .....	8
2.1 Eliminación del ACL creada en el ejercicio anterior .....	9
2.2 Ejecución FTP al Servidor desde uno de los PC's de la Red A .....	9
2.3 Definir el protocolo, qué fuente, qué destino y qué puerto son rechazados.....	9
2.4 Aplicar la ACL a la interfaz .....	10
2.5 Explique ¿Por qué es necesario poner access-list 101 permit ip any? .....	11
2.6 Comprobaciones: .....	11
Repita los pasos del Apartado 2.2 . Ejecute FTP al Servidor desde uno de los PC's de la Red A. ¿Qué sucede? .....	11
Compruebe si se puede hacer FTP al servidor desde un PC de la Red B. ¿Qué observa?.....	11
EJERCICIO 3: VPN con Ipsec Modo Túnel .....	12
1. Objetivo .....	12
2. Crear la topología de la Red.....	12
2.1 Creación de la topología .....	12
2.2 Verificación de la conectividad .....	13
3. VPN y Encriptación .....	14
4. Monitorización y Pruebas .....	17
4.1 Desde el modo simulación envíe un paquete desde uno de los PC's de la red A a uno de los PC's de la red B .....	17
4.2 Verifique si la configuración está funcionando correctamente.....	21
4.3 ¿Qué sucede si configuramos de nuevo el router B, pero cambiamos en esta ocasión la clave vpnuser por otra?.....	21

Ejercicio 1: Listas de acceso estándar

1.1 Crear la topología de la Red

Para ello, comencemos en crear la topología de nuestra red, que es de la siguiente manera:



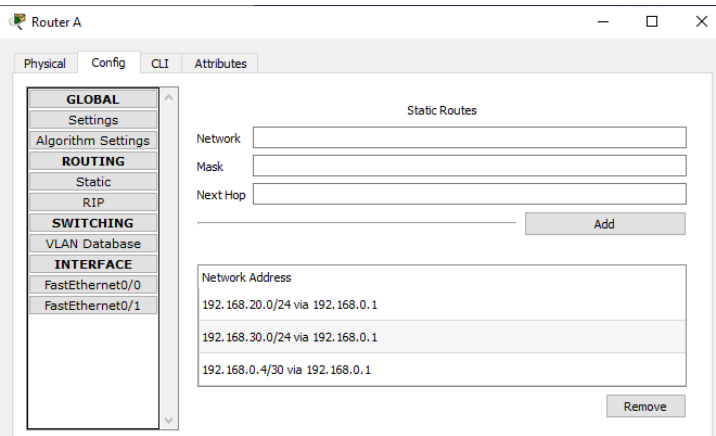
1.2 Configuración de Interfaces, esquema de direccionamiento y tablas de enrutamiento

Disponemos de la siguiente tabla para distinguir bien la configuración de la topología de la red:

NOMBRE	INTERFAZ	DIRECCIÓN IP	MÁSCARA DE RED	GATEWAY
Router INTERNET	FastEthernet 0 0	192.168.0.1	255.255.255.252	-----
	FastEthernet 0 1	192.168.0.5	255.255.255.252	-----
Router A	FastEthernet 0 0	192.168.10.1	255.255.255.0	-----
	FastEthernet 0 1	192.168.0.2	255.255.255.252	-----
Router B	FastEthernet 0 0	192.168.0.6	255.255.255.252	-----
	FastEthernet 0 1	192.168.20.1	255.255.255.0	-----
	Ethernet 0 0	192.168.30.1	255.255.255.0	-----
PC0	FastEthernet 0 0	192.168.10.2	255.255.255.0	192.168.10.1
PC1	FastEthernet 0 0	192.168.10.3	255.255.255.0	192.168.10.1
PC2	FastEthernet 0 0	192.168.20.2	255.255.255.0	192.168.20.1
PC3	FastEthernet 0 0	192.168.20.3	255.255.255.0	192.168.20.1
Server0	FastEthernet 0 0	192.168.30.2	255.255.255.0	192.168.30.1

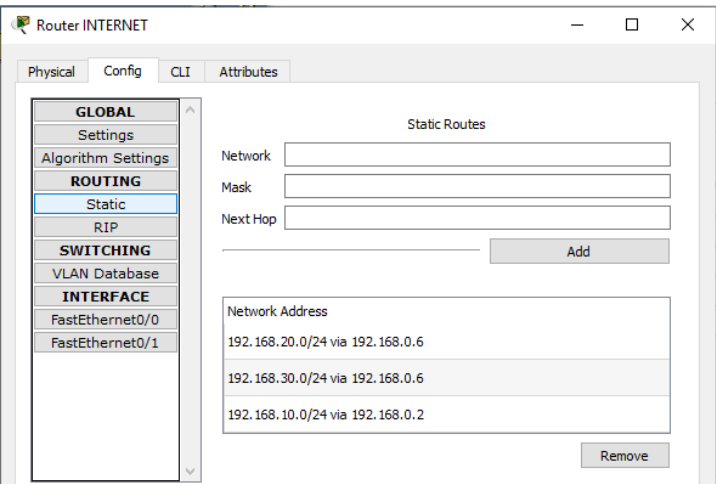
Ahora para conseguir la conectividad entre los equipos, configuraremos las tablas de enrutamiento de cada router mediante el protocolo RIP de la siguiente manera:

En el router A, tenemos las siguientes rutas estáticas y su posterior tabla de enrutamiento:



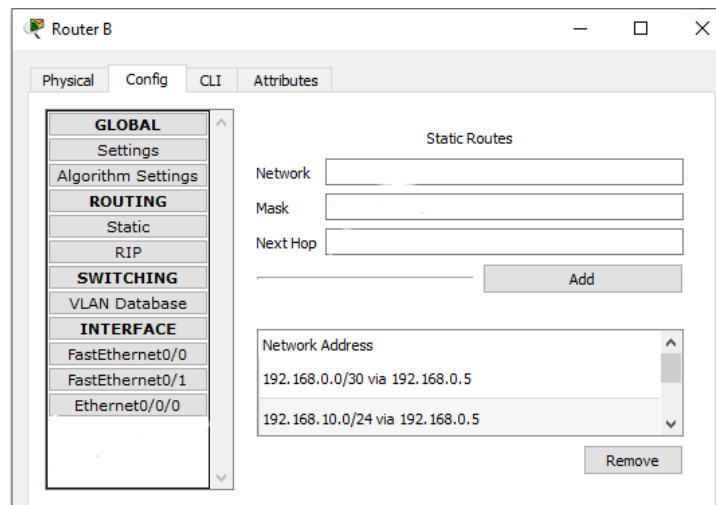
Routing Table for Router A				
Type	Network	Port	Next Hop IP	Metric
C	192.168.0.0/30	FastEthernet0/1	---	0/0
R	192.168.0.4/30	FastEthernet0/1	192.168.0.1	120/1
C	192.168.10.0/24	FastEthernet0/0	---	0/0
R	192.168.20.0/24	FastEthernet0/1	192.168.0.1	120/2
R	192.168.30.0/24	FastEthernet0/1	192.168.0.1	120/2

En el router Internet, tenemos las siguientes rutas estáticas y su posterior tabla de enrutamiento:



Routing Table for Router INTERNET				
Type	Network	Port	Next Hop IP	Metric
C	192.168.0.0/30	FastEthernet0/0	---	0/0
C	192.168.0.4/30	FastEthernet0/1	---	0/0
R	192.168.10.0/24	FastEthernet0/0	192.168.0.2	120/1
R	192.168.20.0/24	FastEthernet0/1	192.168.0.6	120/1
R	192.168.30.0/24	FastEthernet0/1	192.168.0.6	120/1

En el router B, tenemos las siguientes rutas estáticas y su posterior tabla de enrutamiento:



Routing Table for Router B				
Type	Network	Port	Next Hop IP	Metric
S	192.168.0.0/30	---	192.168.0.5	1/0
C	192.168.0.4/30	FastEthernet0/0	---	0/0
S	192.168.10.0/24	---	192.168.0.5	1/0
C	192.168.20.0/24	FastEthernet0/1	---	0/0
C	192.168.30.0/24	Ethernet0/0/0	---	0/0

Con respecto a la tabla de enrutamiento, cabe mencionar que las rutas de tipo C, son aquellas a las que son vecinas con el propio router, y las de tipo R, son aquellas que se ha aplicado el protocolo RIP, que son evidentemente las rutas estáticas aplicadas en las capturas de al lado.

### 1.3 Verificación de la conectividad

Ahora comprobemos la correspondiente conectividad:

Con respecto al PC0, tenemos lo siguiente:

PDU List Window									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	PC1	ICMP		0.000	N	0	(edit)
	Successful	PC0	Router A	ICMP		0.000	N	1	(edit)
	Successful	PC0	Router INTERNET	ICMP		0.000	N	2	(edit)
	Successful	PC0	Router B	ICMP		0.000	N	3	(edit)
	Successful	PC0	PC2	ICMP		0.000	N	4	(edit)
	Successful	PC0	PC3	ICMP		0.000	N	5	(edit)
	Successful	PC0	Server0	ICMP		0.000	N	6	(edit)

Con respecto a PC1, tenemos lo siguiente:

PDU List Window									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC1	PC0	ICMP		0.000	N	0	(edit)
	Successful	PC1	Router A	ICMP		0.000	N	1	(edit)
	Successful	PC1	Router INTERNET	ICMP		0.000	N	2	(edit)
	Successful	PC1	Router B	ICMP		0.000	N	3	(edit)
	Successful	PC1	PC2	ICMP		0.000	N	4	(edit)
	Successful	PC1	PC3	ICMP		0.000	N	5	(edit)
	Successful	PC1	Server0	ICMP		0.000	N	6	(edit)

Con respecto a Router A:

PDU List Window									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	Router A	PC0	ICMP		0.000	N	0	(edit)
	Successful	Router A	PC1	ICMP		0.000	N	1	(edit)
	Successful	Router A	Router INTERNET	ICMP		0.000	N	2	(edit)
	Successful	Router A	Router B	ICMP		0.000	N	3	(edit)
	Successful	Router A	PC2	ICMP		0.000	N	4	(edit)
	Successful	Router A	PC3	ICMP		0.000	N	5	(edit)
	Successful	Router A	Server0	ICMP		0.000	N	6	(edit)

Con respecto a Router Internet:

PDU List Window									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	Router IN...	PC0	ICMP		0.000	N	0	(edit)
	Successful	Router IN...	PC1	ICMP		0.000	N	1	(edit)
	Successful	Router IN...	Router A	ICMP		0.000	N	2	(edit)
	Successful	Router IN...	Router B	ICMP		0.000	N	3	(edit)
	Successful	Router IN...	PC2	ICMP		0.000	N	4	(edit)
	Successful	Router IN...	PC3	ICMP		0.000	N	5	(edit)
	Successful	Router IN...	Server0	ICMP		0.000	N	6	(edit)

Con respecto a Router B:

PDU List Window									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	Router B	PC0	ICMP		0.000	N	0	(edit)
	Successful	Router B	PC1	ICMP		0.000	N	1	(edit)
	Successful	Router B	Router A	ICMP		0.000	N	2	(edit)
	Successful	Router B	Router INTERNET	ICMP		0.000	N	3	(edit)
	Successful	Router B	PC2	ICMP		0.000	N	4	(edit)
	Successful	Router B	PC3	ICMP		0.000	N	5	(edit)
	Successful	Router B	Server0	ICMP		0.000	N	6	(edit)

Con respecto a PC2:

PDU List Window									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC2	PC0	ICMP		0.000	N	0	(edit)
	Successful	PC2	PC1	ICMP		0.000	N	1	(edit)
	Successful	PC2	Router A	ICMP		0.000	N	2	(edit)
	Successful	PC2	Router INTERNET	ICMP		0.000	N	3	(edit)
	Successful	PC2	Router B	ICMP		0.000	N	4	(edit)
	Successful	PC2	PC3	ICMP		0.000	N	5	(edit)
	Successful	PC2	Server0	ICMP		0.000	N	6	(edit)

Con respecto a PC3:

PDU List Window									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC3	PC0	ICMP		0.000	N	0	(edit)
	Successful	PC3	PC1	ICMP		0.000	N	1	(edit)
	Successful	PC3	Router A	ICMP		0.000	N	2	(edit)
	Successful	PC3	Router INTERNET	ICMP		0.000	N	3	(edit)
	Successful	PC3	Router B	ICMP		0.000	N	4	(edit)
	Successful	PC3	PC2	ICMP		0.000	N	5	(edit)
	Successful	PC3	Server0	ICMP		0.000	N	6	(edit)

Con respecto a Server0:

PDU List Window									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	Server0	PC0	ICMP		0.000	N	0	(edit)
	Successful	Server0	PC1	ICMP		0.000	N	1	(edit)
	Successful	Server0	Router A	ICMP		0.000	N	2	(edit)
	Successful	Server0	Router INTERNET	ICMP		0.000	N	3	(edit)
	Successful	Server0	Router B	ICMP		0.000	N	4	(edit)
	Successful	Server0	PC2	ICMP		0.000	N	5	(edit)
	Successful	Server0	PC3	ICMP		0.000	N	6	(edit)

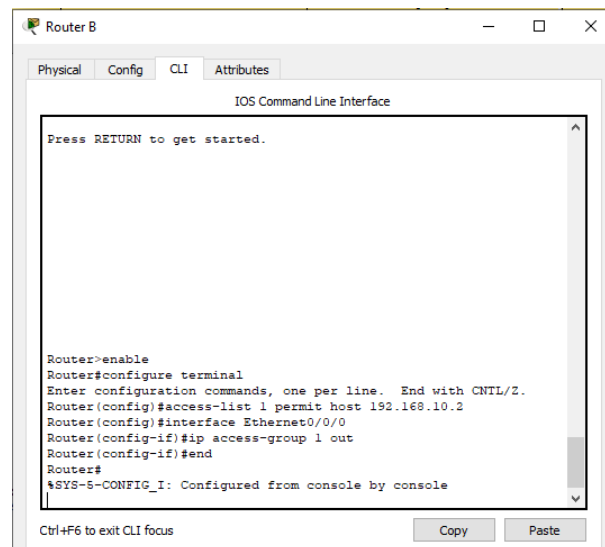
Después de todo esto, concluimos que funciona correctamente.

Para mantener la configuración de todos los equipos, aunque realicemos cambios posteriores, ejecutamos el siguiente comando: Router# *copy running-config startup-config*.

#### 1.4 Configuración Lista de control de acceso estándar

**Objetivo:** Configurar una lista de control de acceso estándar para filtrar los paquetes que llegan al servidor Server0 de manera que solo PC0 de la Red A tenga el acceso permitido, denegando el acceso al resto; para ello hay que aplicar la lista de acceso en la interfaz del router cercana al destino.

Es decir, hay que definir un ACL (lista de acceso estándar) que sólo permita a PC0 (IP: 192.168.10.2) tener acceso al servidor 0 (IP: 192.168.30.2). Para ello en el CLI del router B, escribimos los siguientes comandos:



Lo que hemos hecho es crear una lista de control de acceso (ACL) con un identificador 1, en la que sólo se permite el acceso a la subred 192.168.30.0/24 del router B desde el PC0. Lo que hace que si otro host quisiera enviar un mensaje a ese destino, el paquete será descartado, ya que no le hemos asignado esos permisos o mejor dicho no tienen exactamente la misma dirección IP del PC0. Después, dentro de la subred 192.168.30.0/24, especificamos a la interfaz Ethernet 0|0|0, ya que es donde se nos sitúa el servidor. Y por último, hemos especificado, que únicamente podrá salir de la interfaz Ethernet 0|0|0, aquel paquete cuya dirección IP sea la del origen, en cuyo caso, la del PC0 (192.168.10.2).

## 1.5 Comprobación de la conectividad entre todos los equipos (ping)

¿Podemos acceder al servidor desde todos los equipos?

Como vemos en la siguiente imagen, solamente hay conectividad entre el PC0 – Server0 y viceversa.

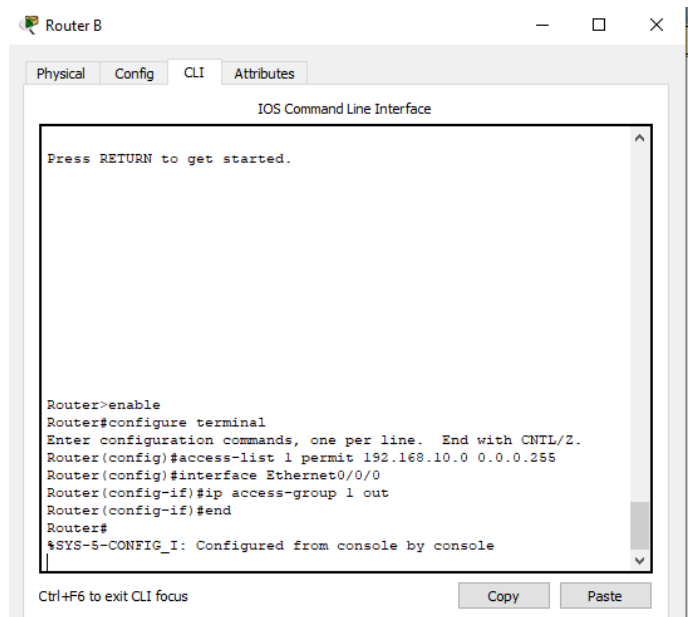
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	Server0	ICMP		0.000	N	0	(edit)
	Failed	PC1	Server0	ICMP		0.000	N	1	(edit)
	Failed	PC2	Server0	ICMP		0.000	N	2	(edit)
	Failed	PC3	Server0	ICMP		0.000	N	3	(edit)
	Successful	Server0	PC0	ICMP		0.000	N	4	(edit)
	Failed	Server0	PC1	ICMP		0.000	N	5	(edit)
	Failed	Server0	PC2	ICMP		0.000	N	6	(edit)
	Failed	Server0	PC3	ICMP		0.000	N	7	(edit)

Lo que nos lleva a la siguiente conclusión:

PC0 envía un paquete al servidor, el router examina si tiene los permisos, en caso contrario, será descartado. Pero, si hacemos el proceso inverso..., es decir, un mensaje desde el servidor al PC0, ¿qué es lo que ocurre? El servidor envía un mensaje al PC0, cuando le llegue al PC0, el responderá con otro mensaje hacia el servidor. De esta manera, como PC0 tiene los permisos, entonces habrá conectividad. De esta manera, está demostrado que desde los dos lados, hay conexión. En cambio, si fuera otro host, como no le hemos aplicado esos permisos, el paquete se descartará en ambos sentidos.

1.6 ¿Qué cambio deberíamos de hacer en la ACL para permitir a toda y solamente a la Red A?

Para ello en el CLI del router B, escribimos los siguientes comandos:



El único cambio que habría que hacer es que en lugar de que solamente tuviera un host en concreto los permisos para enviar un mensaje a un servidor, ahora tenemos una subred. ¿Y esto cómo se consigue? Se consigue mediante la dirección IP de la subred junto con la máscara wildcard. ¿Qué es la máscara wildcard? Es una máscara de bits que nos indican qué direcciones IP son las que tienen o no los permisos en la lista de control de acceso (ACL). Obtenemos la máscara wildcard invirtiendo la máscara de la subred en particular. En este caso, como la máscara de red de la subred A es 255.255.255.0, nos sale que la máscara wildcard es la siguiente: 0.0.0.255. En cuanto al resto es exactamente igual, es decir, la ACL 1 se aplica para que permita salir de la interfaz Ethernet 0|0|0 solamente a los paquetes de la subred A y deniegue el resto del tráfico.

En la siguiente imagen, vemos que solamente de la subred A al servidor y viceversa, funciona correctamente:

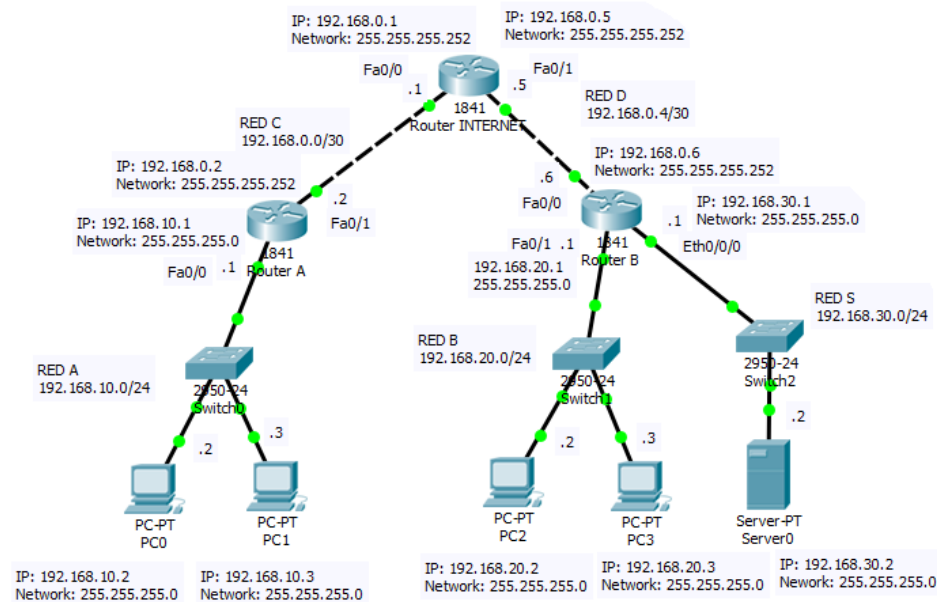
PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	Server0	ICMP		0.000	N	0	(edit)
	Successful	PC1	Server0	ICMP		0.000	N	1	(edit)
	Failed	PC2	Server0	ICMP		0.000	N	2	(edit)
	Failed	PC3	Server0	ICMP		0.000	N	3	(edit)
	Successful	Server0	PC0	ICMP		0.000	N	4	(edit)
	Successful	Server0	PC1	ICMP		0.000	N	5	(edit)
	Failed	Server0	PC2	ICMP		0.000	N	6	(edit)
	Failed	Server0	PC3	ICMP		0.000	N	7	(edit)



## 1.7 ¿Podemos aplicar esa ACL a otra interfaz del router B? ¿Por qué o por qué no?

Depende de la posición en la cual apliquemos el ACL en la interfaz del router B. Para entenderlo mejor, visualicemos de nuevo la topología:



Si aplicamos un ACL a la interfaz FastEthernet 0/0 del router B, resulta que si un host (con los permisos adecuados) envía un paquete al servidor, se llevará a cabo correctamente. Pero sino tiene los permisos necesarios, o bien que el destino no sea el servidor, podría hacer que el paquete se descartase incluso si quisiera acceder a la red B. Para eso se resolvería aplicando otra ACL para la interfaz de la red B.

Si aplicamos un ACL a la interfaz FastEthernet 0/1 del router B, resulta que, si nuestro propósito es mantener vigilado el tráfico hacia el servidor, sería inconsistente aplicar esa ACL asociada a esa interfaz. Serviría si se aplicaría otra ACL para un host específico de esa red B, en cuyo caso se permitiría el tráfico o no, dependiendo del caso.

Conclusión: Cada ACL está asociada a una interfaz, y puede ser de entrada o salida dependiendo del caso relativo. Así que, si queremos analizar el tráfico, tendrá que ser dependiendo de su interfaz y de la manera que queramos que realice.

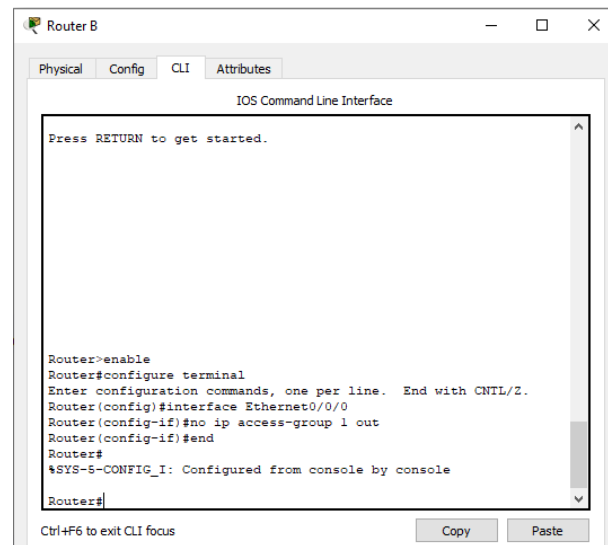
### Ejercicio 2: LISTAS DE ACCESO EXTENDIDA

Siguiendo con el esquema de red, se desea en esta ocasión crear una lista de acceso extendida que impida el tráfico FTP desde la RED A, pero que permita cualquier otro tipo de tráfico.

Dato: FTP usa TCP en los puertos 20 y 21.

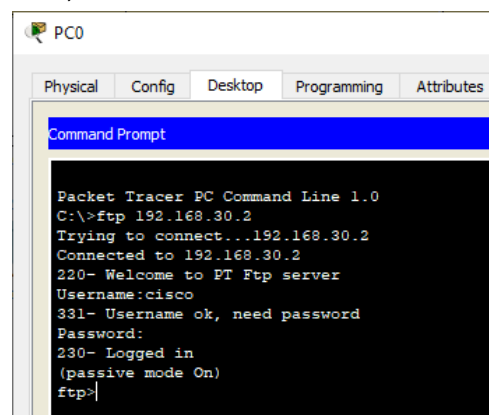
## 2.1 Eliminación del ACL creada en el ejercicio anterior

Para ello en el CLI del router B, escribimos los siguientes comandos:



## 2.2 Ejecución FTP al Servidor desde uno de los PC's de la Red A

Tomemos uno de los PC's de la subred A de utilidad, por ejemplo, el PC0. Escribimos en su terminal el siguiente comando: [ftp 192.168.30.2](#). Después, nos pedirán que introduzcamos un usuario y una contraseña, la cual será cisco. Una vez realizado lo anterior, obtenemos la siguiente imagen:



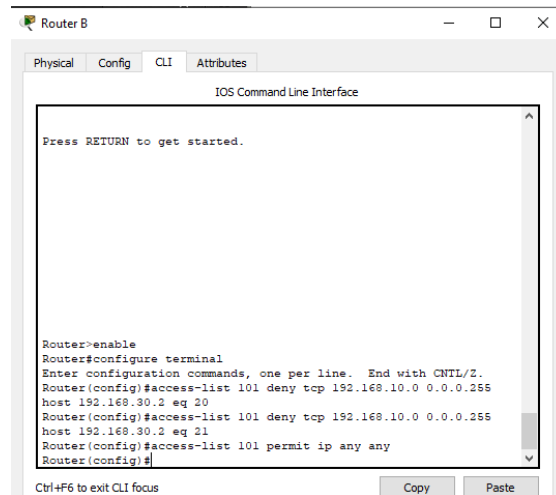
## 2.3 Definir el protocolo, qué fuente, qué destino y qué puerto son rechazados

Hay que impedir el tráfico FTP procedente de la red A al servidor, el resto de las redes si podrán. Debido a que queremos restringir el tráfico de la red A, tendremos que usar las ACL extensas. Las sintaxis que se aplica es la siguiente:

```
access-list access-list-number {permit | deny} protocol source {source-mask}  
destination {destination-mask} [eq destination-port]
```

```
ip access-group access-list-number {in | out}
```

Estas listas tienen asociadas un valor numérico (identificador) que va de un rango desde 100 a 199 y de 2000 a 2699. Por ejemplo, vamos a tomar el 101. Y se cheque tanto la dirección fuente como la dirección destino, y se puede especificar el protocolo (UDP, TCP, IP) y el puerto destino. Una vez sabido esto, como tenemos que denegar la conexión FTP de la red A, tendríamos que realizar los siguientes comandos desde el router B que es el que corresponde con el servidor:



```
Router B
Physical Config CLI Attributes
IOS Command Line Interface

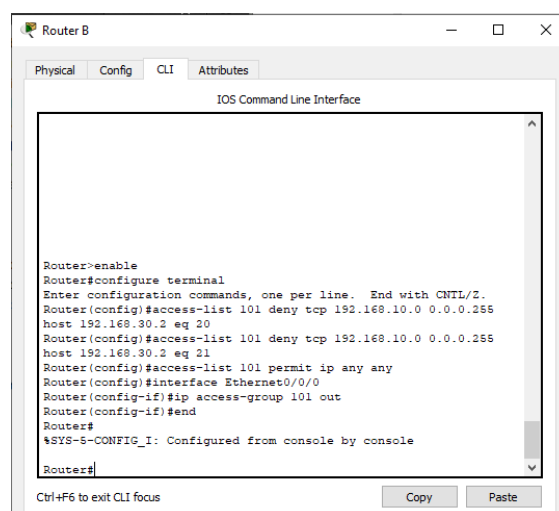
Press RETURN to get started.

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 101 deny tcp 192.168.10.0 0.0.0.255
host 192.168.30.2 eq 20
Router(config)#access-list 101 deny tcp 192.168.10.0 0.0.0.255
host 192.168.30.2 eq 21
Router(config)#access-list 101 permit ip any any
Router(config)#
```

Repetimos, una vez hecho eso, lo que hacemos es impedir el envío de paquetes de cuyo origen sea una dirección IP y su máscara procedente a la subred A (192.168.10.0, 255.255.255.0), además del protocolo TCP en los puertos 20 y 21 (FTP). Pero todo lo demás está permitido el envío de paquetes.

## 2.4 Aplicar la ACL a la interfaz

Aplicaremos la ACL extendida en la interfaz Ethernet 0/0/0, la cual, se aplicará para paquetes que no provengan de la subred A y que no usen el protocolo TCP con los puertos 20 y 21 de destino (FTP). En el caso en el que sea así, se descartará el paquete. Es lo mismo de antes, se que le añadimos las dos siguientes líneas:

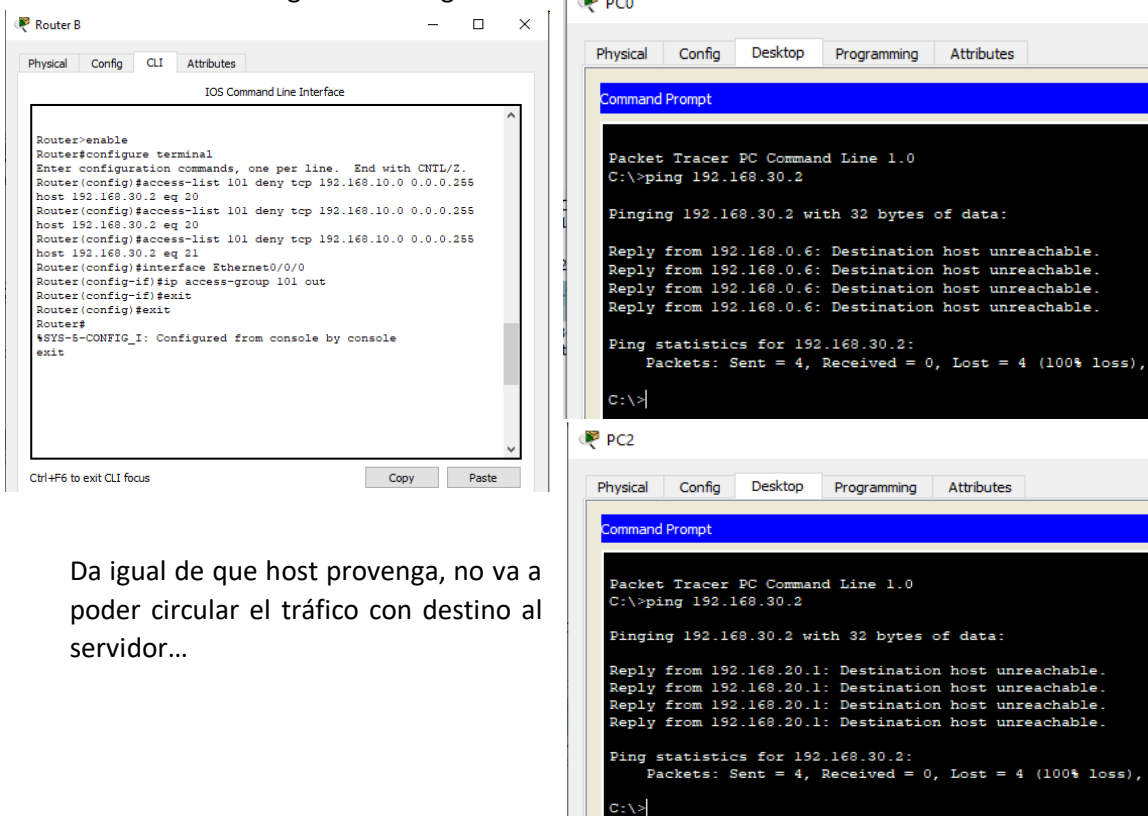


```
Router B
Physical Config CLI Attributes
IOS Command Line Interface

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 101 deny tcp 192.168.10.0 0.0.0.255
host 192.168.30.2 eq 20
Router(config)#access-list 101 deny tcp 192.168.10.0 0.0.0.255
host 192.168.30.2 eq 21
Router(config)#access-list 101 permit ip any any
Router(config)#interface Ethernet0/0/0
Router(config-if)#ip access-group 101 out
Router(config-if)#end
Router#
%SYS-S-CONFIG_I: Configured from console by console
Router#
```

## 2.5 Explique ¿Por qué es necesario poner access-list 101 permit ip any?

Debido a que si aplicamos una ACL extendida, tenemos que indicar qué tráfico queremos que no circule y cuál queremos que sí circule. Para ello, pusimos que no dejara pasar el tráfico TCP procedente de la subred A, por los puertos 20 y 21 (FTP). Y por su supuesto, hay que especificar que el resto del tráfico de otras subredes, sí que podrán hacerlo, es decir, distinguimos del tráfico que sí que se permite del que no se permite. Y eso se consigue gracias a la línea de: "access-list 101 permit ip any". En el caso en que no aparecería esta línea en la terminal del router, provocaríamos la denegación del todo el tráfico. Un ejemplo de esto, lo podemos encontrar en las siguientes imágenes:

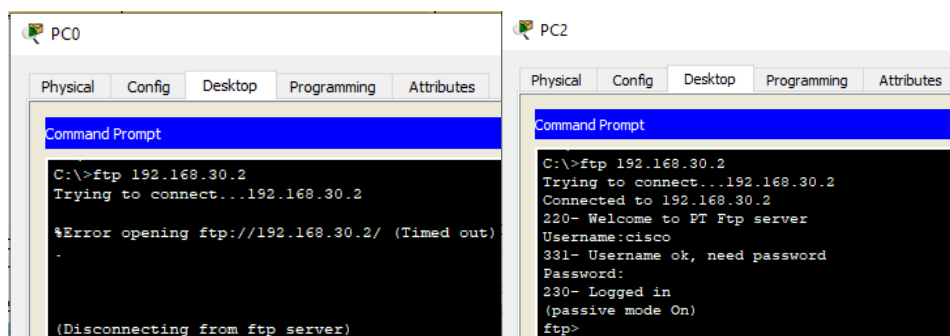


Da igual de que host provenga, no va a poder circular el tráfico con destino al servidor...

## 2.6 Comprobaciones:

Repita los pasos del Apartado 2.2 . Ejecute FTP al Servidor desde uno de los PC's de la Red A. ¿Qué sucede?

Compruebe si se puede hacer FTP al servidor desde un PC de la Red B. ¿Qué observa?



Si cogemos uno de los dos hosts de la subred A, por ejemplo el PC0, vemos claramente que no funciona la conexión FTP. Y si cogemos uno de los dos hosts de la subred B, por ejemplo el PC2, vemos claramente que sí funciona la conexión FTP. Como vemos ha aplicado correctamente el ACL extendida, ya que no deja pasar el tráfico FTP de la subred A ya que utiliza TCP en los puertos 20 y 21, y eso, los hemos denegado. Y por el resto de la red, como si hemos hecho que se circule el tráfico, entonces tenemos que funciona la conexión FTP con el servidor.

### EJERCICIO 3: VPN con Ipsec Modo Túnel

#### 1. Objetivo

Crear una red privada virtual (VPN) utilizando Packet Tracer simulando una conexión entre dos redes pertenecientes a una empresa RED A y RED B y que tiene conexión a Internet, a través del Router 0.

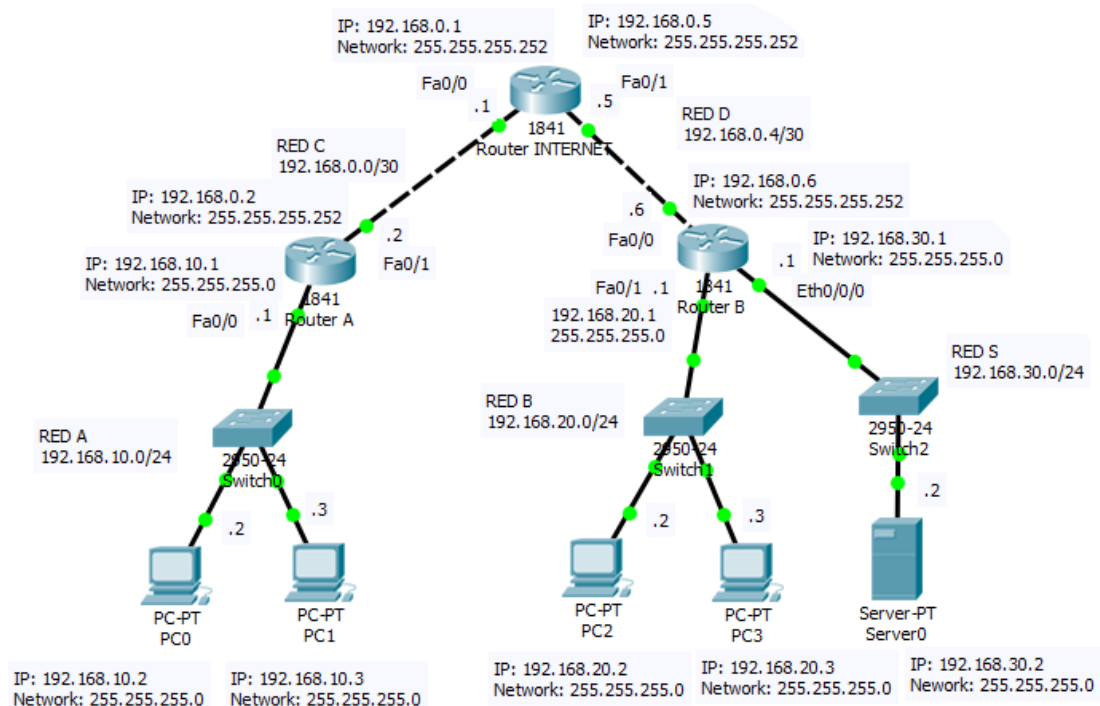
Se debe permitir a los equipos de la RED A tener acceso a los equipos de la RED B y viceversa, pero se desea que las comunicaciones entre dichas redes se realicen con integridad y confidencialidad.

Para ello se utilizará encriptación y autenticación de datos entre las dos áreas utilizando Ipsec modo túnel.

#### 2. Crear la topología de la Red

##### 2.1 Creación de la topología

Vamos a trabajar con la misma topología de utilizada anteriormente, solo que no lleva ningún tipo de listas de control de acceso.



## 2.2 Verificación de la conectividad

Ahora vamos a comprobar la conectividad:

Con respecto a PC0:

PDU List Window									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	Router A	ICMP		0.000	N	0	(edit)
	Successful	PC0	Router INTERNET	ICMP		0.000	N	1	(edit)
	Successful	PC0	Router B	ICMP		0.000	N	2	(edit)
	Successful	PC0	PC2	ICMP		0.000	N	3	(edit)
	Successful	PC0	PC3	ICMP		0.000	N	4	(edit)
	Successful	PC0	Server0	ICMP		0.000	N	5	(edit)

Con respecto a PC1:

PDU List Window									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC1	PC0	ICMP		0.000	N	0	(edit)
	Successful	PC1	Router A	ICMP		0.000	N	1	(edit)
	Successful	PC1	Router INTERNET	ICMP		0.000	N	2	(edit)
	Successful	PC1	Router B	ICMP		0.000	N	3	(edit)
	Successful	PC1	PC2	ICMP		0.000	N	4	(edit)
	Successful	PC1	PC3	ICMP		0.000	N	5	(edit)
	Successful	PC1	Server0	ICMP		0.000	N	6	(edit)

Con respecto a Router A:

PDU List Window									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	Router A	PC0	ICMP		0.000	N	0	(edit)
	Successful	Router A	PC1	ICMP		0.000	N	1	(edit)
	Successful	Router A	Router INTERNET	ICMP		0.000	N	2	(edit)
	Successful	Router A	Router B	ICMP		0.000	N	3	(edit)
	Successful	Router A	PC2	ICMP		0.000	N	4	(edit)
	Successful	Router A	PC3	ICMP		0.000	N	5	(edit)
	Successful	Router A	Server0	ICMP		0.000	N	6	(edit)

Con respecto a Router Internet:

PDU List Window									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	Router IN...	PC0	ICMP		0.000	N	0	(edit)
	Successful	Router IN...	PC1	ICMP		0.000	N	1	(edit)
	Successful	Router IN...	Router A	ICMP		0.000	N	2	(edit)
	Successful	Router IN...	Router B	ICMP		0.000	N	3	(edit)
	Successful	Router IN...	PC2	ICMP		0.000	N	4	(edit)
	Successful	Router IN...	PC3	ICMP		0.000	N	5	(edit)
	Successful	Router IN...	Server0	ICMP		0.000	N	6	(edit)

Con respecto a Router B:

PDU List Window									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	Router B	PC0	ICMP		0.000	N	0	(edit)
	Successful	Router B	PC1	ICMP		0.000	N	1	(edit)
	Successful	Router B	Router A	ICMP		0.000	N	2	(edit)
	Successful	Router B	Router INTERNET	ICMP		0.000	N	3	(edit)
	Successful	Router B	PC2	ICMP		0.000	N	4	(edit)
	Successful	Router B	PC3	ICMP		0.000	N	5	(edit)
	Successful	Router B	Server0	ICMP		0.000	N	6	(edit)

Con respecto a PC2:

PDU List Window									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC2	PC0	ICMP		0.000	N	0	(edit)
	Successful	PC2	PC1	ICMP		0.000	N	1	(edit)
	Successful	PC2	Router A	ICMP		0.000	N	2	(edit)
	Successful	PC2	Router INTERNET	ICMP		0.000	N	3	(edit)
	Successful	PC2	Router B	ICMP		0.000	N	4	(edit)
	Successful	PC2	PC3	ICMP		0.000	N	5	(edit)
	Successful	PC2	Server0	ICMP		0.000	N	6	(edit)

Con respecto a PC3:

PDU List Window									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC3	PC0	ICMP		0.000	N	0	(edit)
	Successful	PC3	PC1	ICMP		0.000	N	1	(edit)
	Successful	PC3	Router A	ICMP		0.000	N	2	(edit)
	Successful	PC3	Router INTERNET	ICMP		0.000	N	3	(edit)
	Successful	PC3	Router B	ICMP		0.000	N	4	(edit)
	Successful	PC3	PC2	ICMP		0.000	N	5	(edit)
	Successful	PC3	Server0	ICMP		0.000	N	6	(edit)

Con respecto a Server0:

PDU List Window									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	Server0	PC0	ICMP		0.000	N	0	(edit)
	Successful	Server0	PC1	ICMP		0.000	N	1	(edit)
	Successful	Server0	Router A	ICMP		0.000	N	2	(edit)
	Successful	Server0	Router INTERNET	ICMP		0.000	N	3	(edit)
	Successful	Server0	Router B	ICMP		0.000	N	4	(edit)
	Successful	Server0	PC2	ICMP		0.000	N	5	(edit)
	Successful	Server0	PC3	ICMP		0.000	N	6	(edit)

Como vemos la conectividad se realiza correctamente.

### 3. VPN y Encriptación

Una vez configurados todos los equipos adecuadamente y verificado que existe conectividad entre todos ellos, vamos a realizar la encriptación de los paquetes para que las redes A y B realicen comunicaciones con integridad y confidencialidad, es decir, que el resto (Internet) no conozca el contenido de dichos paquetes:

Vamos a realizar los siguientes pasos:

#### Router A

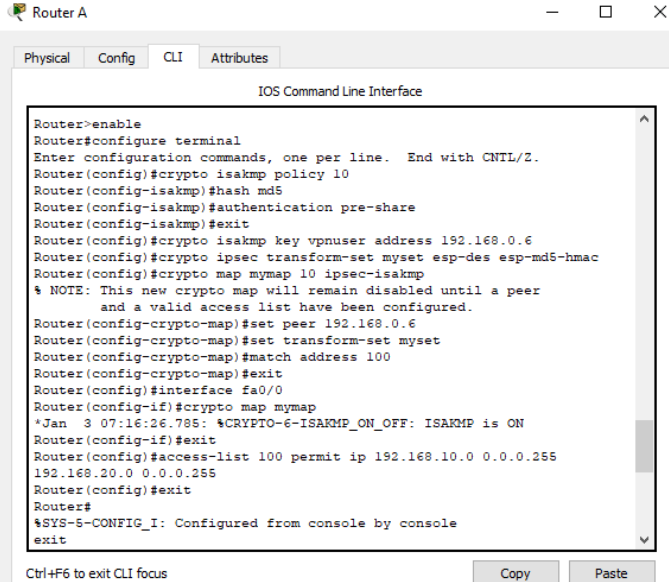
Usaremos los siguientes protocolos:

- Protocolo IPsec (Internet Protocol Security): Es un conjunto de protocolos que se utilizan para proteger las comunicaciones IP. IPsec incluye intercambio de claves y cifrado de túnel. Al crear una VPN IPsec se pueden elegir entre una variedad de tecnologías de seguridad.
- AH (Authentication Header): Proporciona integridad y autenticación, y evita el ataque por repetición.
- ESP (Encrypted Security Payload): Proporciona integridad y autenticación, evita el ataque por repetición y asegura la confidencialidad.
- Protocolo ISAKMP (Internet Security Association and Key Management Protocol): ISAKMP proporciona mecanismos para la autenticación en una comunicación segura

entre hosts. Suele utilizar IKE (Internet Key Exchange), protocolo basado en el intercambio secreto de claves.

- MD5 (Message Digest 5 (Algoritmo de Resumen del Mensaje 5)): es un algoritmo para resumir mensajes de manera criptográficamente segura ampliamente utilizado. La codificación del MD5 de 128 bits se representa típicamente como un número de 32 dígitos hexadecimales.
- SHA: Secure Hash Algorithm. Es un conjunto de funciones de resumen criptográfico diseñado por la Agencia de Seguridad Nacional (NSA). Los algoritmos SHA están estructurados de manera diferente y se distinguen como SHA-0, SHA-1 y SHA-2, en función del número de bits del resumen.
- DES: (Data Encryption Standard): Proporciona cifrado simétrico con una clave de 56-bits. Ya no es considerado un protocolo seguro porque su clave es demasiado corta, lo que lo vuelve vulnerable a ataques de fuerza bruta.
- HMAC (Hashing Message Authentication Code): Es un tipo de código de autenticación de mensajes (MAC). HMAC se calcula mediante un algoritmo específico que incluye una función de resumen criptográfico en combinación con una clave secreta.

Para ello en el CLI de la terminal escribimos lo siguiente:



```
Router A
Physical Config CLI Attributes
IOS Command Line Interface
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#exit
Router(config)#crypto isakmp key vpnuser address 192.168.0.6
Router(config)#crypto ipsec transform-set myset esp-des esp-md5-hmac
Router(config)#crypto map mymap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)#set peer 192.168.0.6
Router(config-crypto-map)#set transform-set myset
Router(config-crypto-map)#match address 100
Router(config-crypto-map)#exit
Router(config)#interface fa0/0
Router(config-if)#crypto map mymap
*Jan 3 07:16:26.785: %CRYPTO-6-ISAAMP_ON_OFF: ISAAMP is ON
Router(config-if)#exit
Router(config)#access-list 100 permit ip 192.168.10.0 0.0.0.255
192.168.20.0 0.0.0.255
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

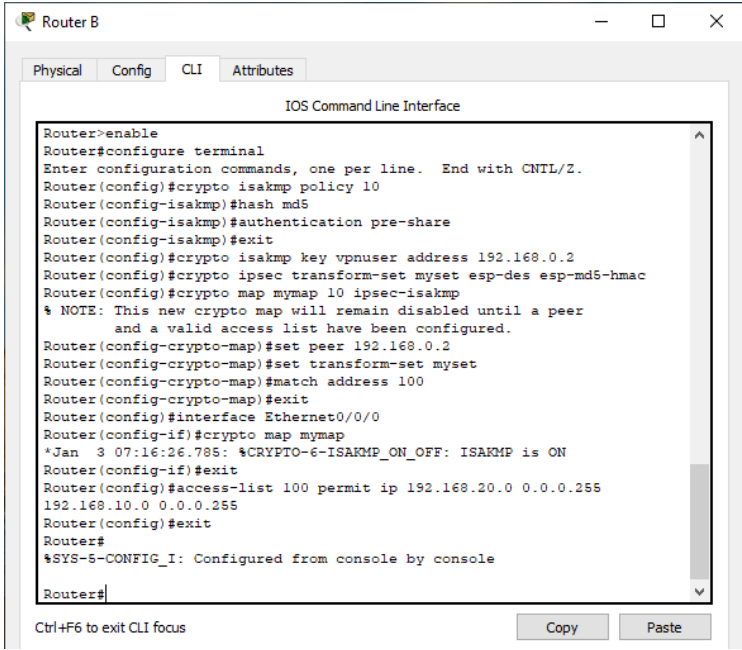
Lo que hacemos en la terminal es lo siguiente:

- “enable”: Habilitamos la terminal del CLI del router A.
- “configure terminal”: Nos introducimos en la configuración de la terminal.
- “crypto isakmp policy 10”: configuramos el protocolo ISAKMP, asignándole un número de prioridad para identificar la política de prioridad de las negociaciones ISAKMP.
- “hash md5”: indicamos el método md5 criptográfico hash.
- “authentication pre-share”: indicamos el método de autenticación por clave acordada.
- “exit”: salida de la configuración.
- “crypto isakmp key vpnuser address 192.168.0.6”: Aplicamos la clave compartida, que en este caso es: “vpnuser”, junto con la dirección del otro par de la conexión, en este caso es el router B (192.168.0.6) de la red D.
- “crypto ipsec transform-set myset esp-des esp-md5-hmac”: Aplicamos un transform-set para saber que políticas de seguridad se aplican durante la conexión.



- “crypto map mymap 10 ipsec-isakmp”: Aplicamos un mapa criptográfico “mymap” vinculado con la política de seguridad aplicada del protocolo isakmp recientemente.
- “set peer 192.168.0.6”: Aplicamos la dirección al otro par al que se está enviando en la conexión.
- “set transform-set myset”: se da como nombre al transform-set creado recientemente como myset.
- “match address 100”: Proporcionamos al mapa criptográfico una ACL de identificador 100.
- “exit”: salida de la configuración.
- “interface fa0/0”: Aplicamos el ACL a la interfaz0/0.
- “crypto map mymap”: Adjuntamos el mapa criptográfico a la interfaz establecida recientemente.
- “exit”: salida de la configuración.
- “Access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255”: Creamos el ACL extendida con un identificador de 100, donde hacemos que permita todo el tráfico con direcciones IP entre las redes C ( IP: 192.168.10.0, Netmask: 255.255.255.0) y D (IP: 192.168.20.0, Netmask: 255.255.255.0) (Router A – Router Internet – Router B).
- “exit”: salida de la configuración.

### **Router B**



```

Router B
Physical Config CLI Attributes
IOS Command Line Interface
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#exit
Router(config)#crypto isakmp key vpnuser address 192.168.0.2
Router(config)#crypto ipsec transform-set myset esp-des esp-md5-hmac
Router(config)#crypto map mymap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)#set peer 192.168.0.2
Router(config-crypto-map)#set transform-set myset
Router(config-crypto-map)#match address 100
Router(config-crypto-map)#exit
Router(config)#interface Ethernet0/0/0
Router(config-if)#crypto map mymap
*Jan 3 07:16:26.785: %CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
Router(config-if)#exit
Router(config)#access-list 100 permit ip 192.168.20.0 0.0.0.255
192.168.10.0 0.0.0.255
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
  
```

En el router B, es exactamente igual que el del router A, salvo a excepción de:

- Cambio de dirección IP de 192.168.0.6 por 192.168.0.2, ya que en este caso, no necesitamos la dirección del propio router B, sino del otro par (router A) para establecer la conexión. Más en concreto en las siguientes líneas: “crypto isakmp key vpnuser address 192.168.0.2” y “set peer 192.168.0.2”.
- Otro cambio sería el de la interfaz, es decir, “interface Ethernet0/0/0”, que ha sido cambiado por el de “interface fa0/0”.

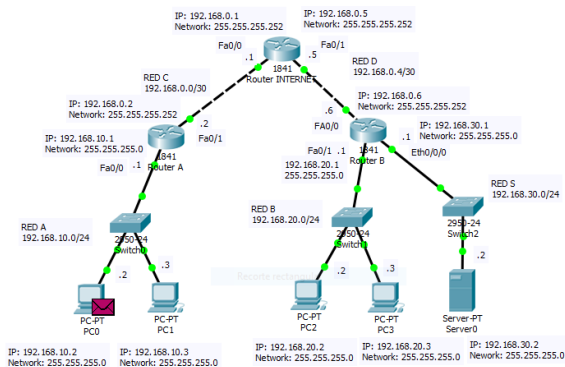
- Otro cambio, en concreto en la ACL, es decir, en: “access-list 100 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255”, antes era de sentido (router A - router B), y ahora es al revés, es decir, (router B - router A).

## 4. Monitorización y Pruebas

### 4.1 Desde el modo simulación enví un paquete desde uno de los PC's de la red A a uno de los PC's de la red B

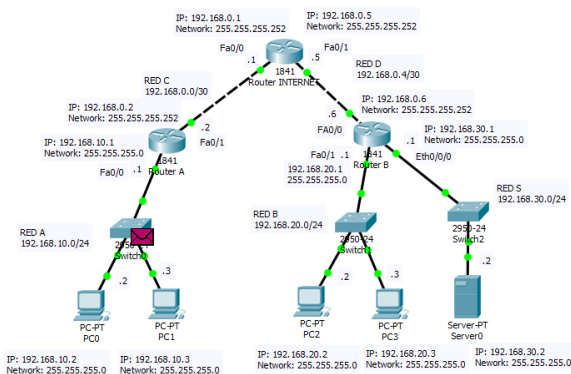
Vamos a enviar paquetes desde PC0 de la red A hacia PC3 de la red B.

#### Situación 1:



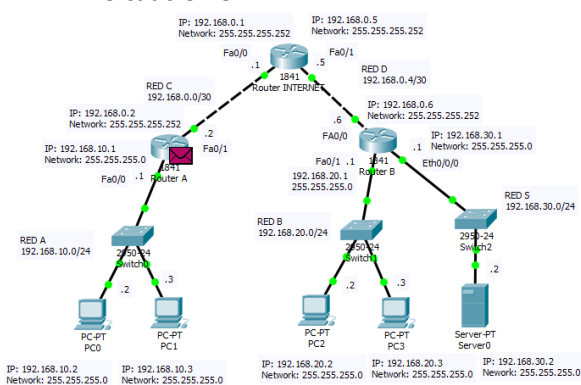
Simulation Panel						
Event List						
Vis.	Time(sec)	Last Device	At Device	Type	Info	
	0.000	--	PC0	ICMP		
	0.001	PC0	Switch0	ICMP		
	0.002	Switch0	Router A	ICMP		
	0.003	Router A	Router IN...	ICMP		
	0.004	Router INT...	Router B	ICMP		
	0.005	Router B	Switch1	ICMP		
	0.006	Switch1	PC2	ICMP		
	0.006	Switch1	PC3	ICMP		
	0.007	PC3	Switch1	ICMP		
Reset Simulation <input checked="" type="checkbox"/> Constant Delay Captured to: 413.137 s						
Play Controls						
Back Auto Capture / Play Capture / Forward						

#### Situación 2:



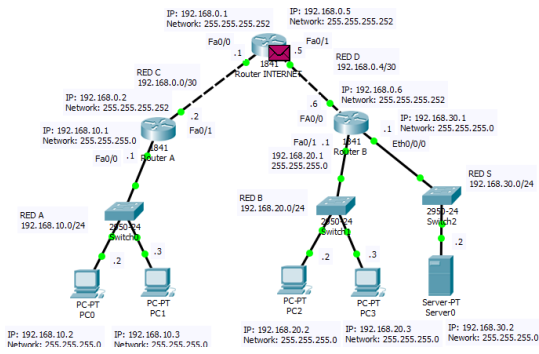
Simulation Panel						
Event List						
Vis.	Time(sec)	Last Device	At Device	Type	Info	
	0.000	--	PC0	ICMP		
	0.001	PC0	Switch0	ICMP		
	0.002	Switch0	Router A	ICMP		
	0.003	Router A	Router IN...	ICMP		
	0.004	Router INT...	Router B	ICMP		
	0.005	Router B	Switch1	ICMP		
	0.006	Switch1	PC2	ICMP		
	0.006	Switch1	PC3	ICMP		
	0.007	PC3	Switch1	ICMP		
Reset Simulation <input checked="" type="checkbox"/> Constant Delay Captured to: 413.137 s						
Play Controls						
Back Auto Capture / Play Capture / Forward						

#### Situación 3:



Simulation Panel						
Event List						
Vis.	Time(sec)	Last Device	At Device	Type	Info	
	0.000	--	PC0	ICMP		
	0.001	PC0	Switch0	ICMP		
	0.002	Switch0	Router A	ICMP		
	0.003	Router A	Router IN...	ICMP		
	0.004	Router INT...	Router B	ICMP		
	0.005	Router B	Switch1	ICMP		
	0.006	Switch1	PC2	ICMP		
	0.006	Switch1	PC3	ICMP		
	0.007	PC3	Switch1	ICMP		
Reset Simulation <input checked="" type="checkbox"/> Constant Delay Captured to: 413.137 s						
Play Controls						
Back Auto Capture / Play Capture / Forward						

### Situación 4:

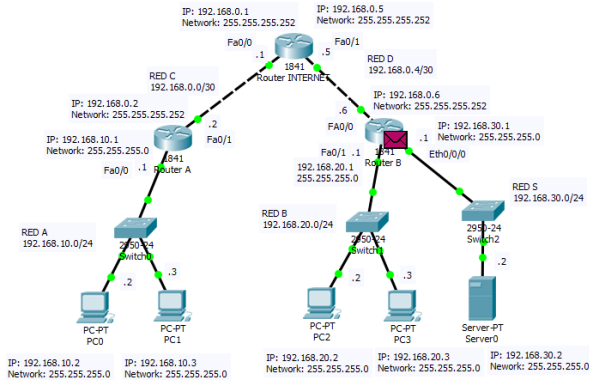


Simulation Panel					
Event List					
Vis.	Time(sec)	Last Device	At Device	Type	Info
0.000	--	PC0	ICMP		
0.001	PC0	Switch0	ICMP		
0.002	Switch0	Router A	ICMP		
0.003	Router A	Router IN...	ICMP		
0.004	Router INT...	Router B	ICMP		
0.005	Router B	Switch1	ICMP		
0.006	Switch1	PC2	ICMP		
0.007	Switch1	PC3	ICMP		

Reset Simulation ☒ Constant Delay Captured to: 413.137 s

Play Controls: Back Auto Capture / Play Capture / Forward

### Situación 5:

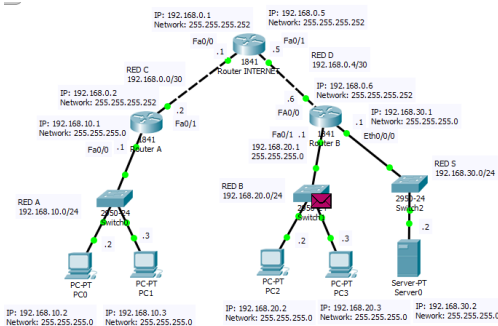


Simulation Panel					
Event List					
Vis.	Time(sec)	Last Device	At Device	Type	Info
0.000	--	PC0	ICMP		
0.001	PC0	Switch0	ICMP		
0.002	Switch0	Router A	ICMP		
0.003	Router A	Router IN...	ICMP		
0.004	Router INT...	Router B	ICMP		
0.005	Router B	Switch1	ICMP		
0.006	Switch1	PC2	ICMP		
0.007	Switch1	PC3	ICMP		

Reset Simulation ☒ Constant Delay Captured to: 413.137 s

Play Controls: Back Auto Capture / Play Capture / Forward

### Situación 6:

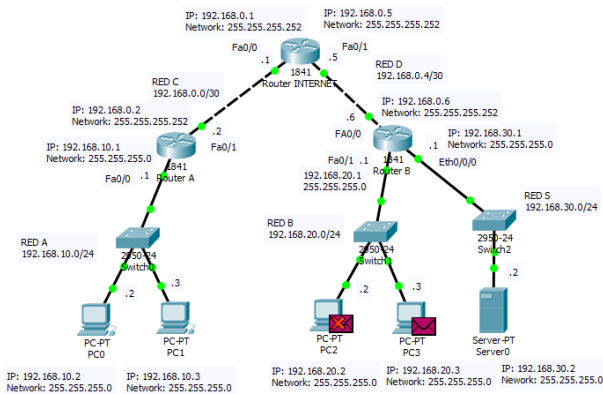


Simulation Panel					
Event List					
Vis.	Time(sec)	Last Device	At Device	Type	Info
0.000	--	PC0	ICMP		
0.001	PC0	Switch0	ICMP		
0.002	Switch0	Router A	ICMP		
0.003	Router A	Router IN...	ICMP		
0.004	Router INT...	Router B	ICMP		
0.005	Router B	Switch1	ICMP		
0.006	Switch1	PC2	ICMP		
0.007	Switch1	PC3	ICMP		

Reset Simulation ☒ Constant Delay Captured to: 413.137 s

Play Controls: Back Auto Capture / Play Capture / Forward

### Situación 7:

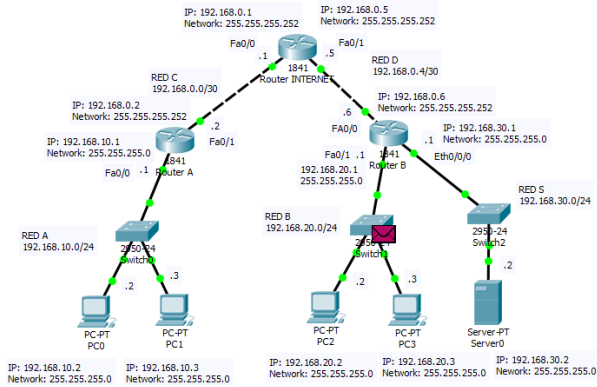


Simulation Panel					
Event List					
Vis.	Time(sec)	Last Device	At Device	Type	Info
0.000	--	PC0	ICMP		
0.001	PC0	Switch0	ICMP		
0.002	Switch0	Router A	ICMP		
0.003	Router A	Router IN...	ICMP		
0.004	Router INT...	Router B	ICMP		
0.005	Router B	Switch1	ICMP		
0.006	Switch1	PC2	ICMP		
0.007	Switch1	PC3	ICMP		

Reset Simulation ☒ Constant Delay Captured to: 413.137 s

Play Controls: Back Auto Capture / Play Capture / Forward

### Situación 8:

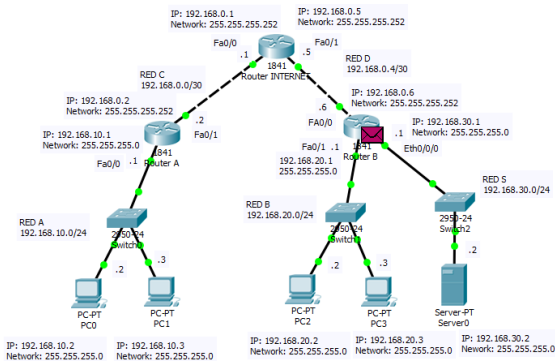


Simulation Panel					
Event List					
Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.005	Router B	Switch1	ICMP	
	0.006	Switch1	PC2	ICMP	
	0.006	Switch1	PC3	ICMP	
	0.007	PC3	Switch1	ICMP	
	0.008	Switch1	Router B	ICMP	
	0.009	Router B	Router IN...	ICMP	
	0.010	Router INT...	Router A	ICMP	
	0.011	Router A	Switch0	ICMP	
	0.012	Switch0	PC0	ICMP	

Reset Simulation ☒ Constant Delay Captured to: 413.137 s

Play Controls: Back Auto Capture / Play Capture / Forward

### Situación 9:

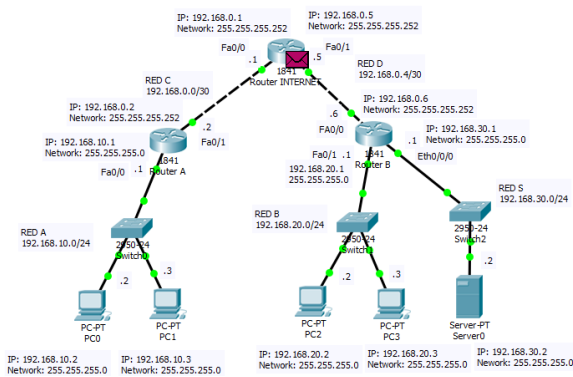


Simulation Panel					
Event List					
Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.005	Router B	Switch1	ICMP	
	0.006	Switch1	PC2	ICMP	
	0.006	Switch1	PC3	ICMP	
	0.007	PC3	Switch1	ICMP	
	0.008	Switch1	Router B	ICMP	
	0.009	Router B	Router IN...	ICMP	
	0.010	Router INT...	Router A	ICMP	
	0.011	Router A	Switch0	ICMP	
	0.012	Switch0	PC0	ICMP	

Reset Simulation ☒ Constant Delay Captured to: 413.137 s

Play Controls: Back Auto Capture / Play Capture / Forward

### Situación 10:

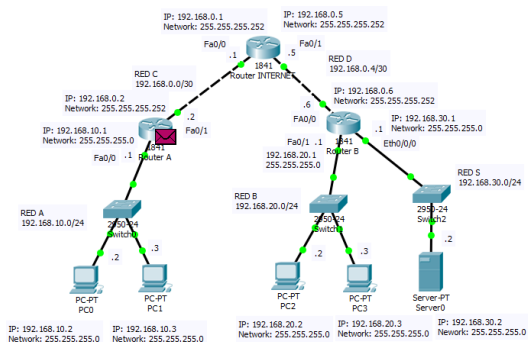


Simulation Panel					
Event List					
Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.005	Router B	Switch1	ICMP	
	0.006	Switch1	PC2	ICMP	
	0.006	Switch1	PC3	ICMP	
	0.007	PC3	Switch1	ICMP	
	0.008	Switch1	Router B	ICMP	
	0.009	Router B	Router IN...	ICMP	
	0.010	Router INT...	Router A	ICMP	
	0.011	Router A	Switch0	ICMP	
	0.012	Switch0	PC0	ICMP	

Reset Simulation ☒ Constant Delay Captured to: 413.137 s

Play Controls: Back Auto Capture / Play Capture / Forward

### Situación 11:

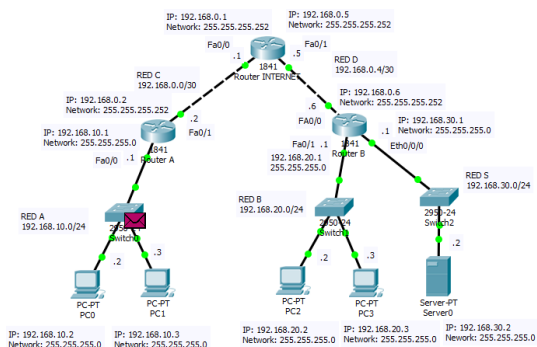


Simulation Panel					
Event List					
Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.005	Router B	Switch1	ICMP	
	0.006	Switch1	PC2	ICMP	
	0.006	Switch1	PC3	ICMP	
	0.007	PC3	Switch1	ICMP	
	0.008	Switch1	Router B	ICMP	
	0.009	Router B	Router IN...	ICMP	
	0.010	Router INT...	Router A	ICMP	
	0.011	Router A	Switch0	ICMP	
	0.012	Switch0	PC0	ICMP	

Reset Simulation ☒ Constant Delay Captured to: 413.137 s

Play Controls: Back Auto Capture / Play Capture / Forward

## Situación 12:

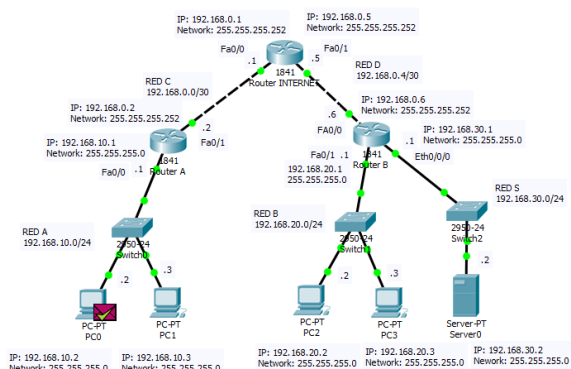


Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.005	Router B	Switch1	ICMP	
	0.006	Switch1	PC2	ICMP	
	0.006	Switch1	PC3	ICMP	
	0.007	PC3	Switch1	ICMP	
	0.008	Switch1	Router B	ICMP	
	0.009	Router B	Router IN...	ICMP	
	0.010	Router INT...	Router A	ICMP	
	0.011	Router A	Switch0	ICMP	
	0.012	Switch0	PC0	ICMP	

Reset Simulation ☒ Constant Delay Captured to: 413.137 s

Play Controls: Back Auto Capture / Play Capture / Forward

## Situación 13:



Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.005	Router B	Switch1	ICMP	
	0.006	Switch1	PC2	ICMP	
	0.006	Switch1	PC3	ICMP	
	0.007	PC3	Switch1	ICMP	
	0.008	Switch1	Router B	ICMP	
	0.009	Router B	Router IN...	ICMP	
	0.010	Router INT...	Router A	ICMP	
	0.011	Router A	Switch0	ICMP	
	0.012	Switch0	PC0	ICMP	

Reset Simulation ☒ Constant Delay Captured to: 413.137 s

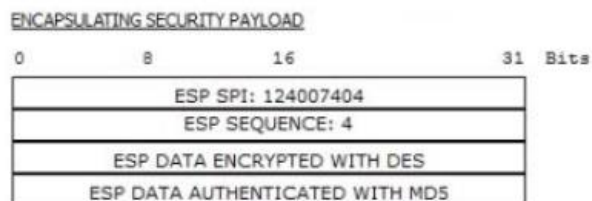
Play Controls: Back Auto Capture / Play Capture / Forward

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	PC3	ICMP		0.000	N	0	(edit)

Por lo que hemos visualizado en las anteriores imágenes, concluimos que se ha realizado correctamente la conectividad entre la red A y la red B.

Si seleccionamos uno de los paquetes de la lista de eventos en los que intervenga Router A o Router B como destino y abrimos la ventana de información de la PDU y en dicha ventana seleccionamos la pestaña “Outbound PDU detail”, nos encontramos la sección de “Encapsulation Security Payload (ESP)”, lo que viene ser la siguiente imagen:



¿Cómo se encapsulan los datos? ¿Cómo se autentican?

Los datos son encapsulados en un paquete de tamaño de 32 bits, donde están encriptados mediante el mecanismo de encriptación de 56 bits y se autentican mediante el MD5.

## 4.2 Verifique si la configuración está funcionando correctamente

Para comprobar el túnel creado utilice el comando **Router# show crypto ipsec sa:**

Desde el router A, obtenemos la siguiente imagen:

```
Router>enable
Router#show crypto ipsec sa

interface: FastEthernet0/0
  Crypto map tag: mymap, local addr 192.168.0.2

protected vrf: (none)
local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
current_peer 192.168.0.6 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 0
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 192.168.0.2, remote crypto endpt.:192.168.0.6
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x076433EC(124007404)

inbound esp sas:
  spi: 0x14840EAF(344198831)
```

Desde el router B, obtenemos la siguiente imagen:

```
Router>enabl
Router#show crypto ipsec sa

interface: FastEthernet0/0
  Crypto map tag: mymap, local addr 192.168.0.6

protected vrf: (none)
local  ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
current_peer 192.168.0.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 0
#pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 192.168.0.6, remote crypto endpt.:192.168.0.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x14840EAF(344198831)

inbound esp sas:
  spi: 0x076433EC(124007404)
```

Utilizar el comando debug para comprobar que se establece un canal seguro, mediante lo siguiente: **Router# debug crypto**

```
Router#debug crypto ipsec
Crypto IPSEC debugging is on
Router#debug crypto isakmp
Crypto ISAKMP debugging is on
Router#
```

## 4.3 ¿Qué sucede si configuramos de nuevo el router B, pero cambiamos en esta ocasión la clave vpnuser por otra?

Cuando un host origen envía un paquete a un host destino al que se está aplicando un protocolo de encriptación, resulta que cualquier router dentro de la ruta, comprueba la clave de cifrado. Si por casualidad, no es la misma que la que tiene que ser, el router rechazará ese paquete. Como ocurre en este caso, hará que el paquete no llegue al destino.