CREACIÓN DE UNA VPN EN PACKET TRACER

Presentado a:

Milton García

Presentado por:

Paula Díaz
Heidy solano
Wilmar Albarracín

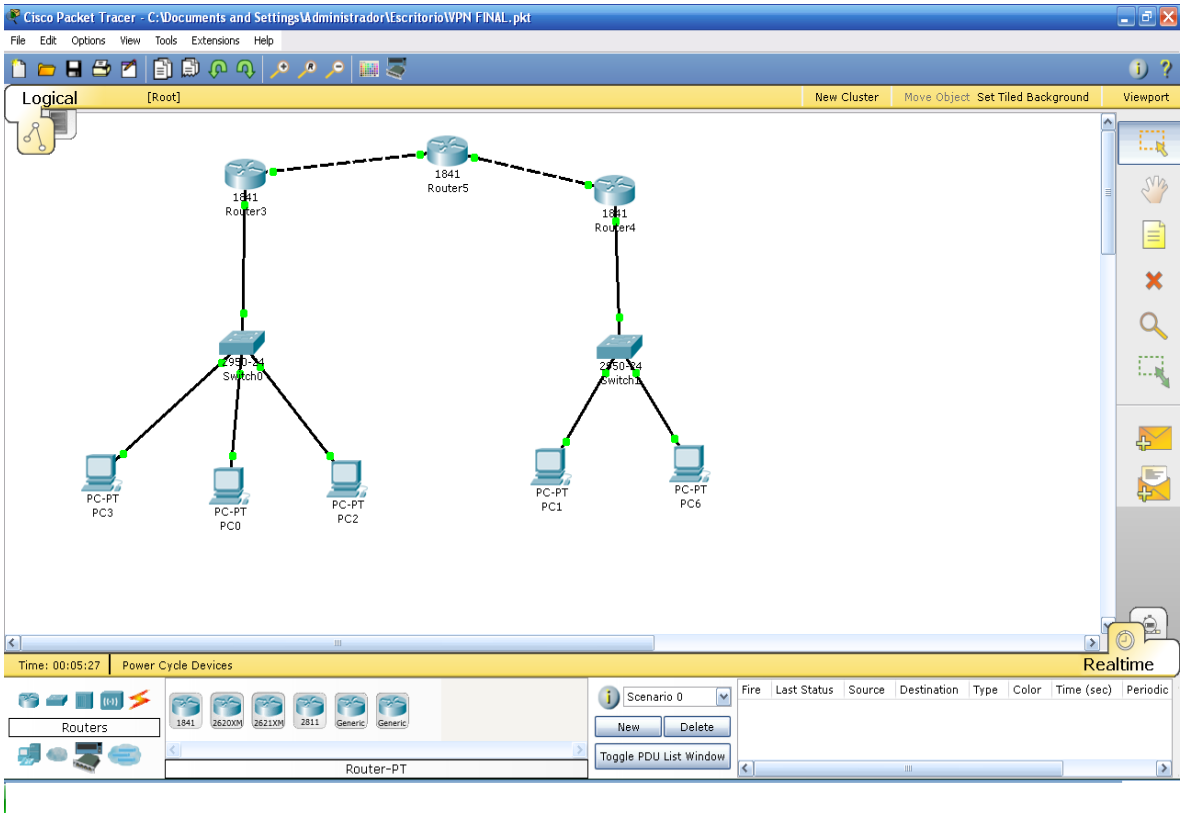
FUNDACION UNIVERSITARIA SAN MARTIN
INGENIERIA DE SISTEMAS
NUEVAS TECONOLOGIAS EN REDES
2010

CREACIÓN DE UNA VPN EN PACKET TRACER

Objetivo:

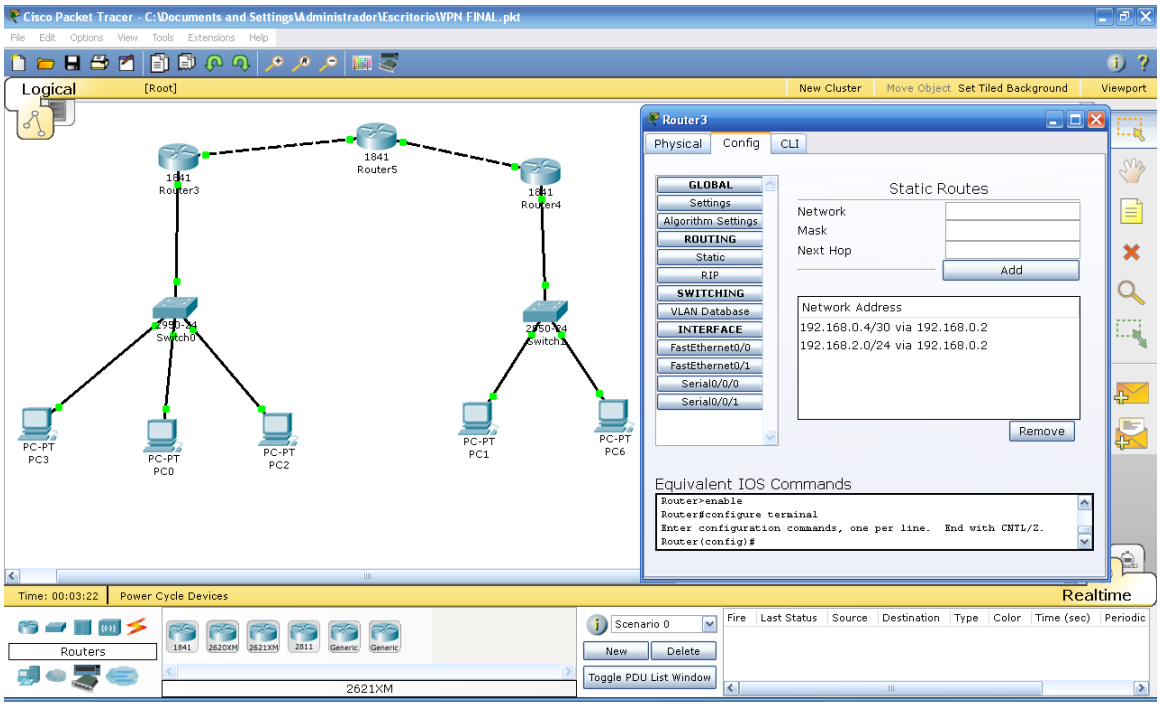
Crear una VPN en Packet Tracer simulando una conexión de dos áreas de una empresa utilizando como vínculo Internet, permitiendo a los miembros de soporte técnico tener acceso a los equipos de cómputo de la otra área. Todo ello utilizando la infraestructura de Internet y una encriptación entre las dos áreas.

A continuación se observara el ejemplo de la VPN:

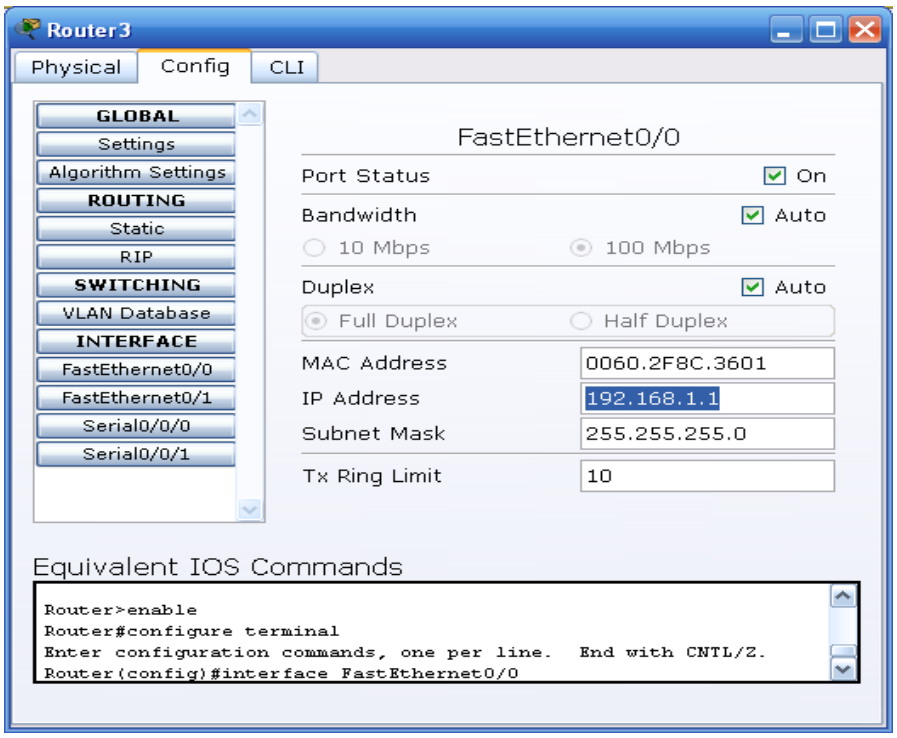


Router 3

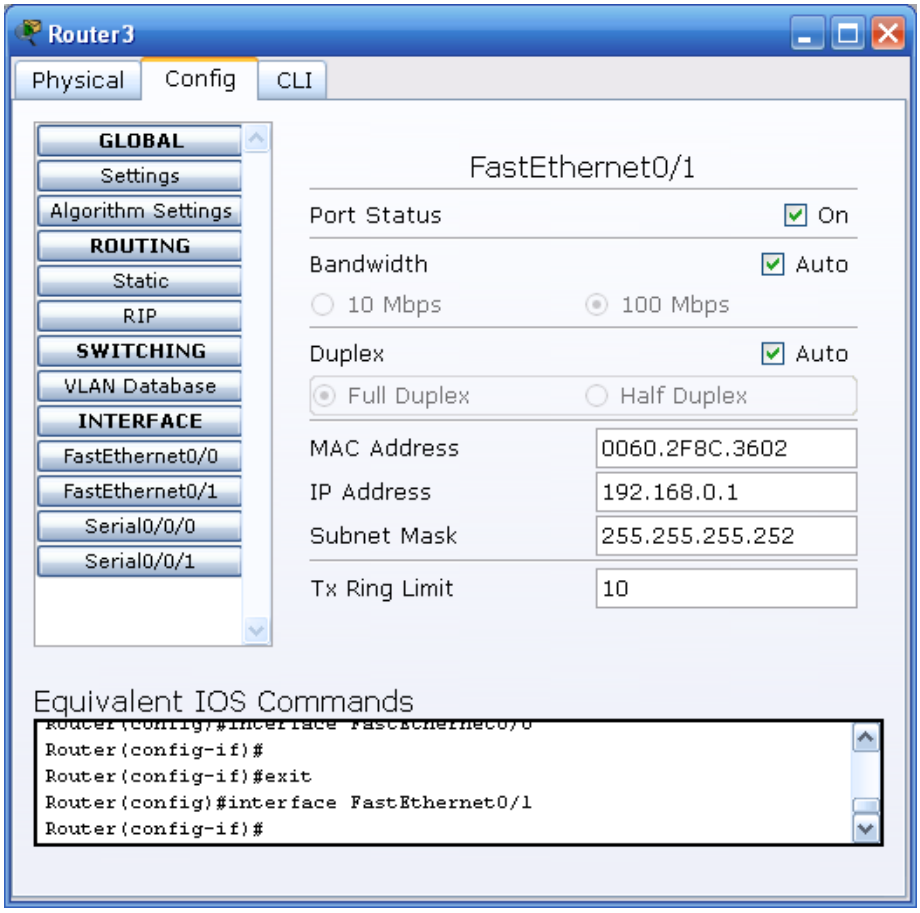
Se comienza por configurar el router 3 especificando el enrutamiento estático: ip origen libre tanto de la WAN como de la LAN y el next hop o siguiente salto a la FastEthernet 0/0 del router 5 o Internet.

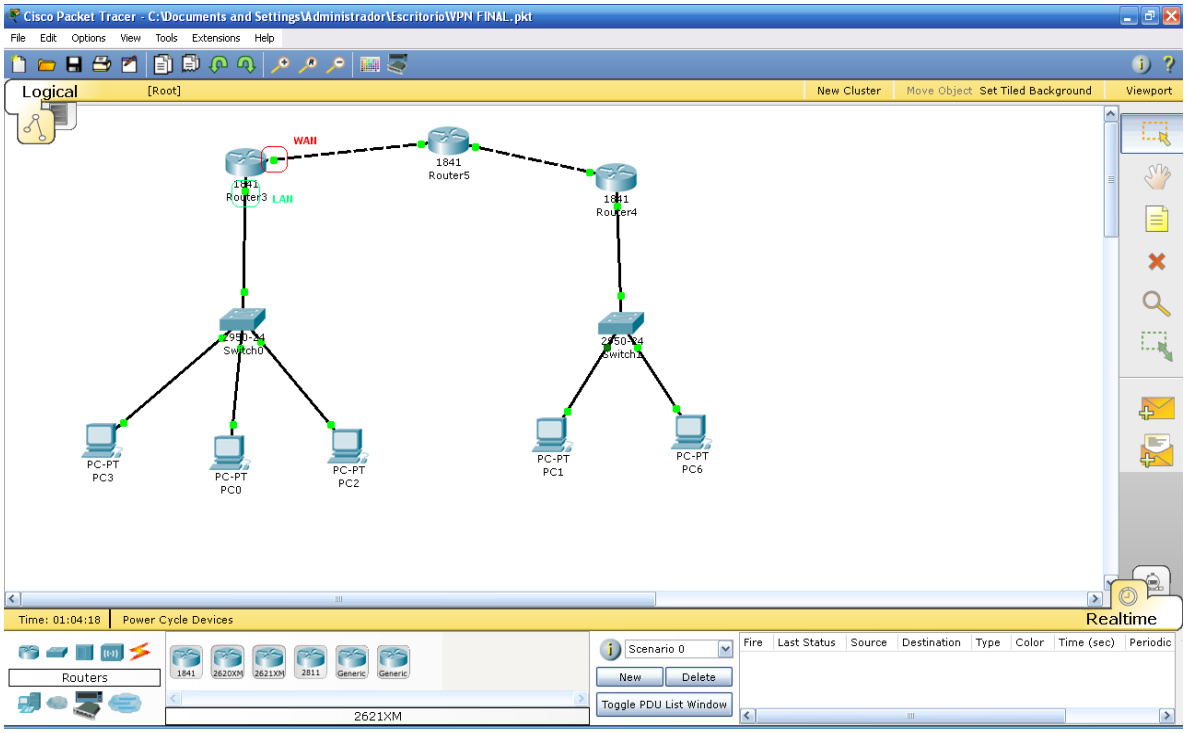


Ahora para la conexión en la parte LAN se encuentra un switch y tres equipos, se configura la interface FastEthernet 0/0 la cual lleva la ip address 192.168.1.1 con una mascara de red 24: 255.255.255.0 :



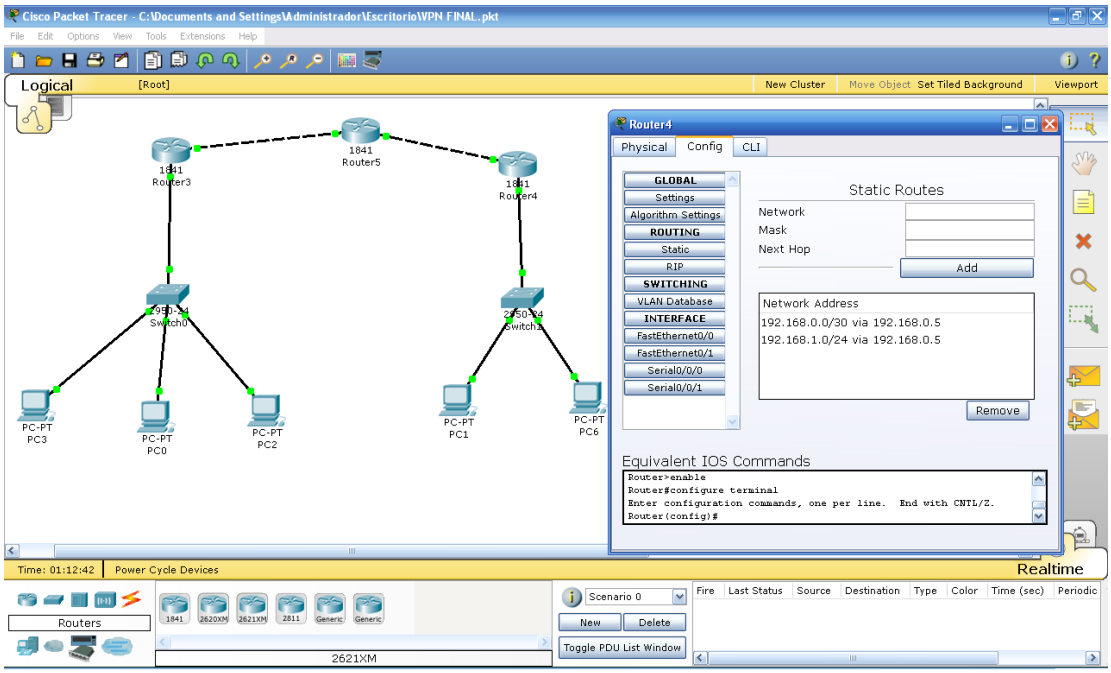
Para la conexión en la parte WAN que va dirigido hacia el router 5 se configura la interface FastEthernet 0/1 la cual lleva la ip address 192.168.0.1 con una mascara de red 30: 255.255.255.252 :



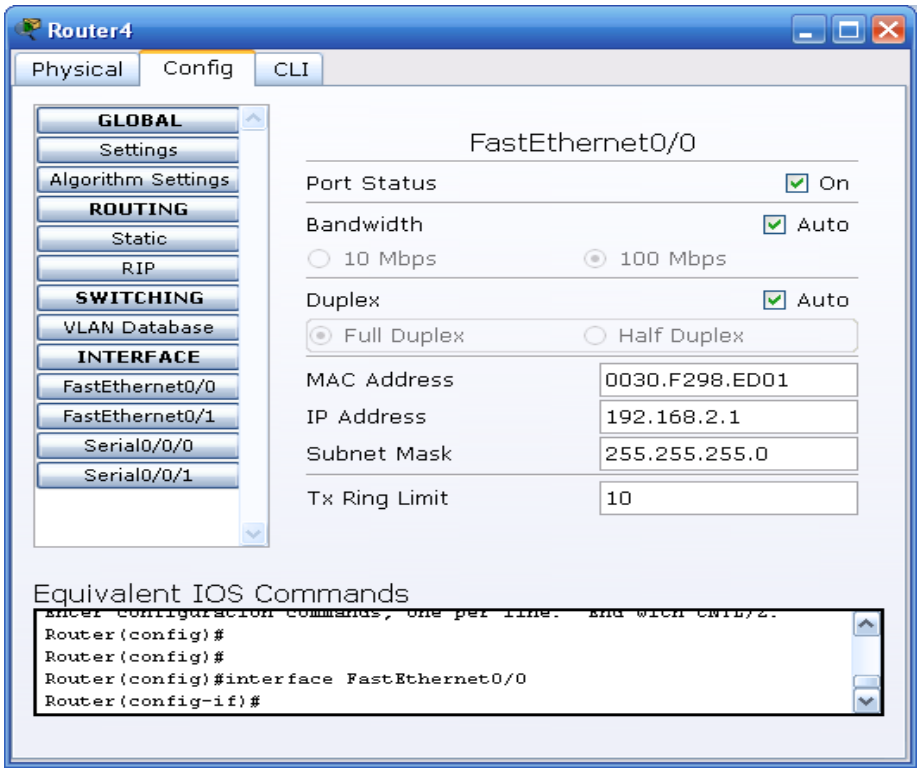


Router 4

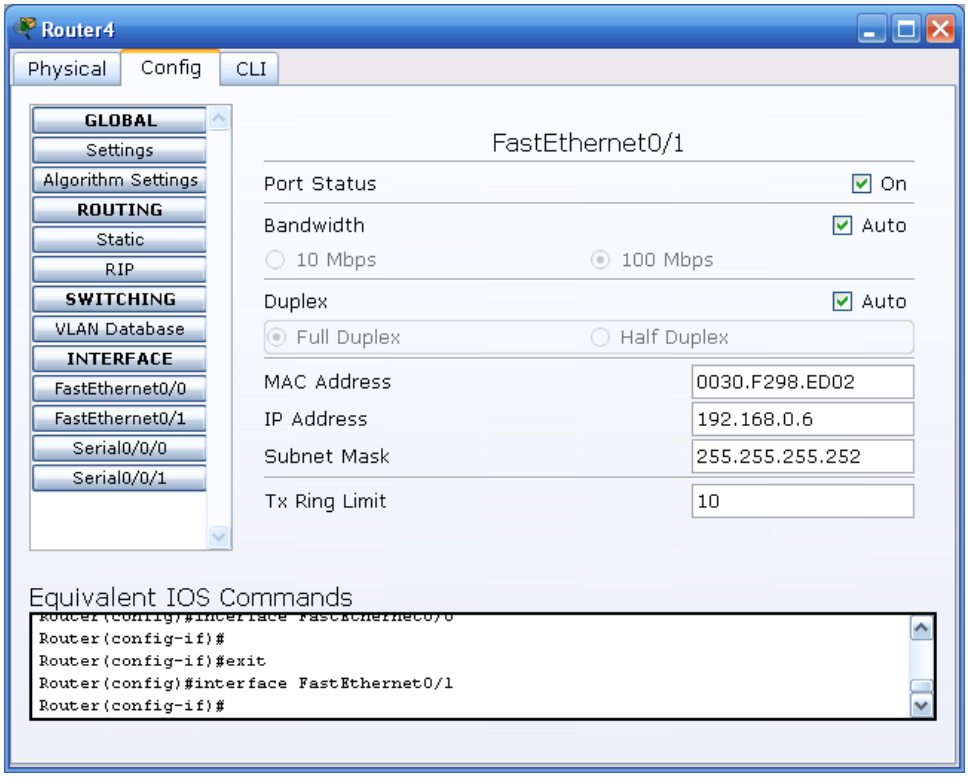
Se configura el router 4 especificando el enrutamiento estático: ip origen libre tanto de WAN (/30) como de LAN (/24) y el next hop o siguiente salto a la FastEthernet 0/1 del router 5 o Internet:

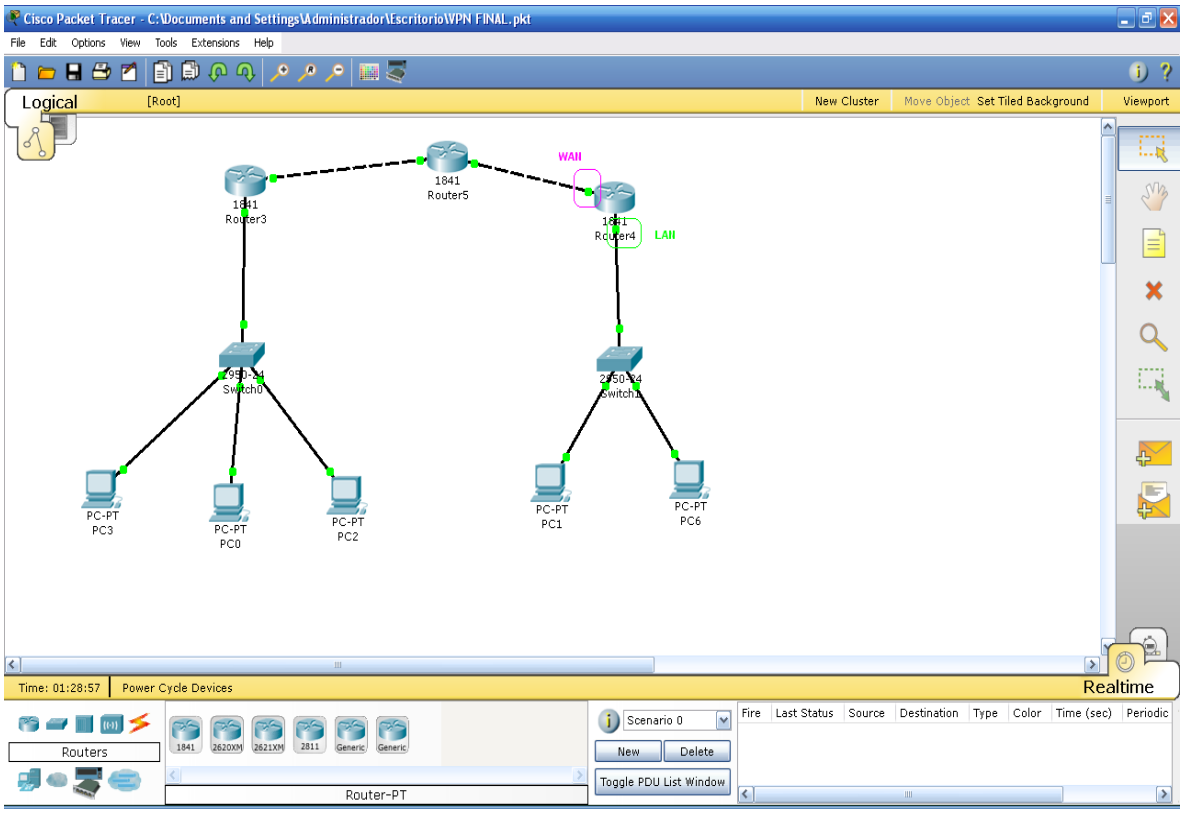


Para la conexión en la parte LAN se encuentra un switch y dos equipos, se configura la interface FastEthernet 0/0 la cual lleva la ip address 192.168.2.1 con una mascara de red 24: 255.255.255.0 :



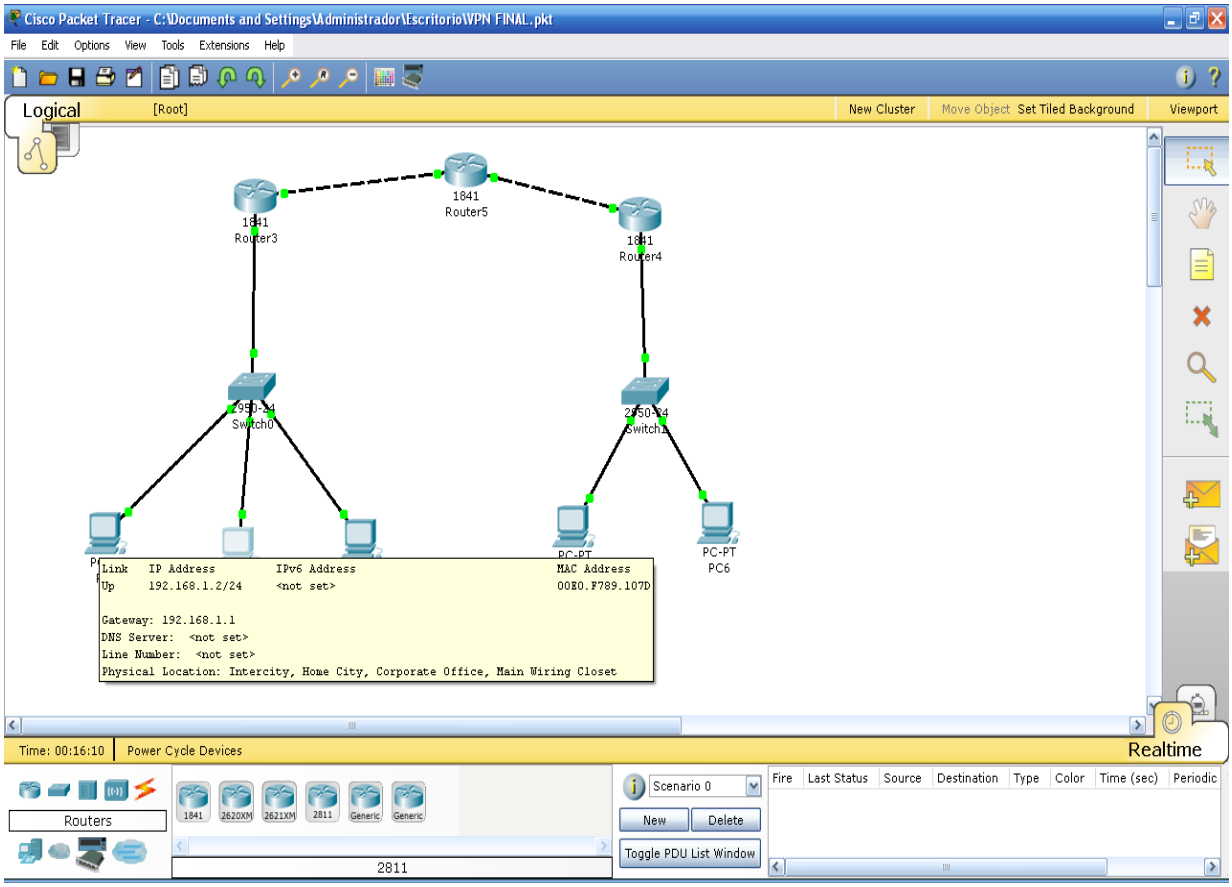
Para la conexión en la parte WAN que va dirigido hacia el router 5 se configura la interface FastEthernet 0/1 la cual lleva la ip address 192.168.0.6 con una mascara de red 30: 255.255.255.252:





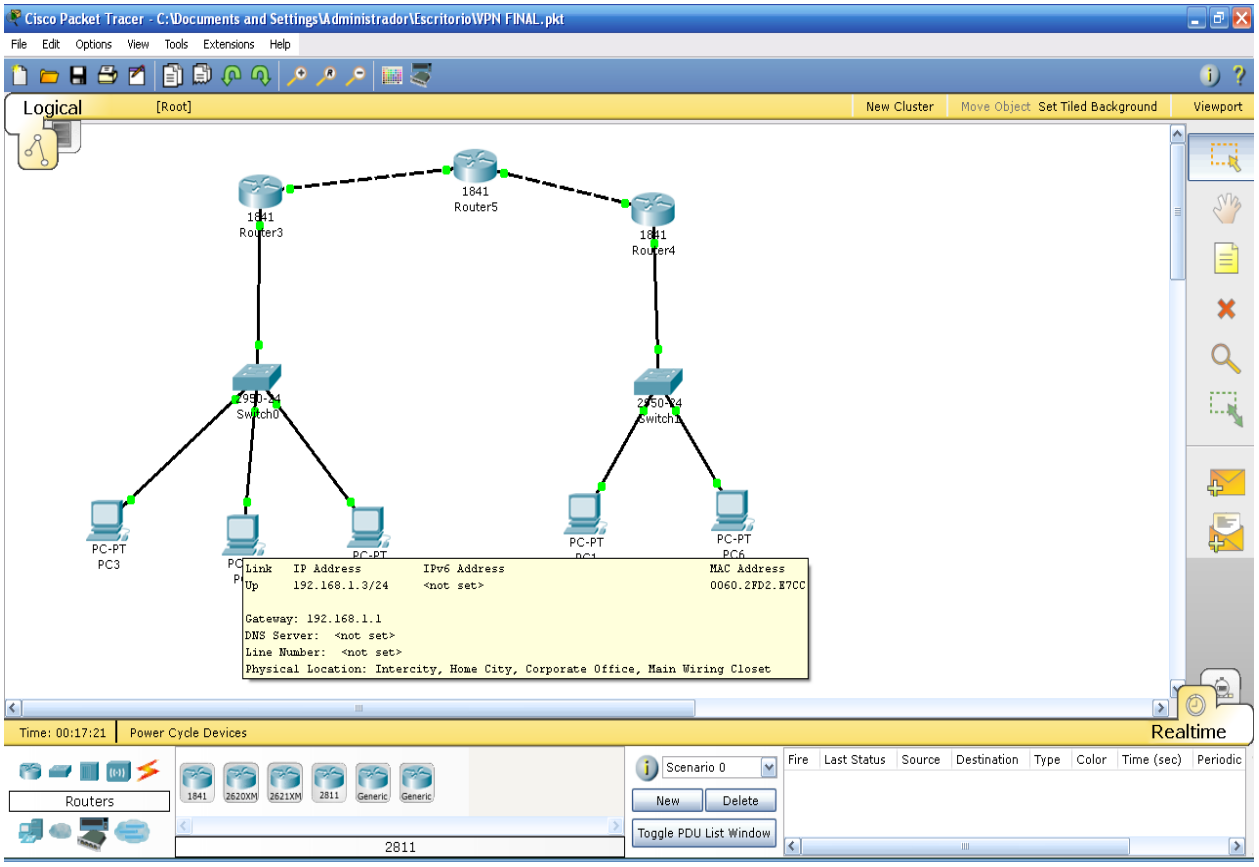
PC 3

En el PC3 de la parte LAN Router 3 se configura el Gateway 192.168.1.1 y la ip address 192.168.1.2 con una mascara de red 24: 255.255.255.0



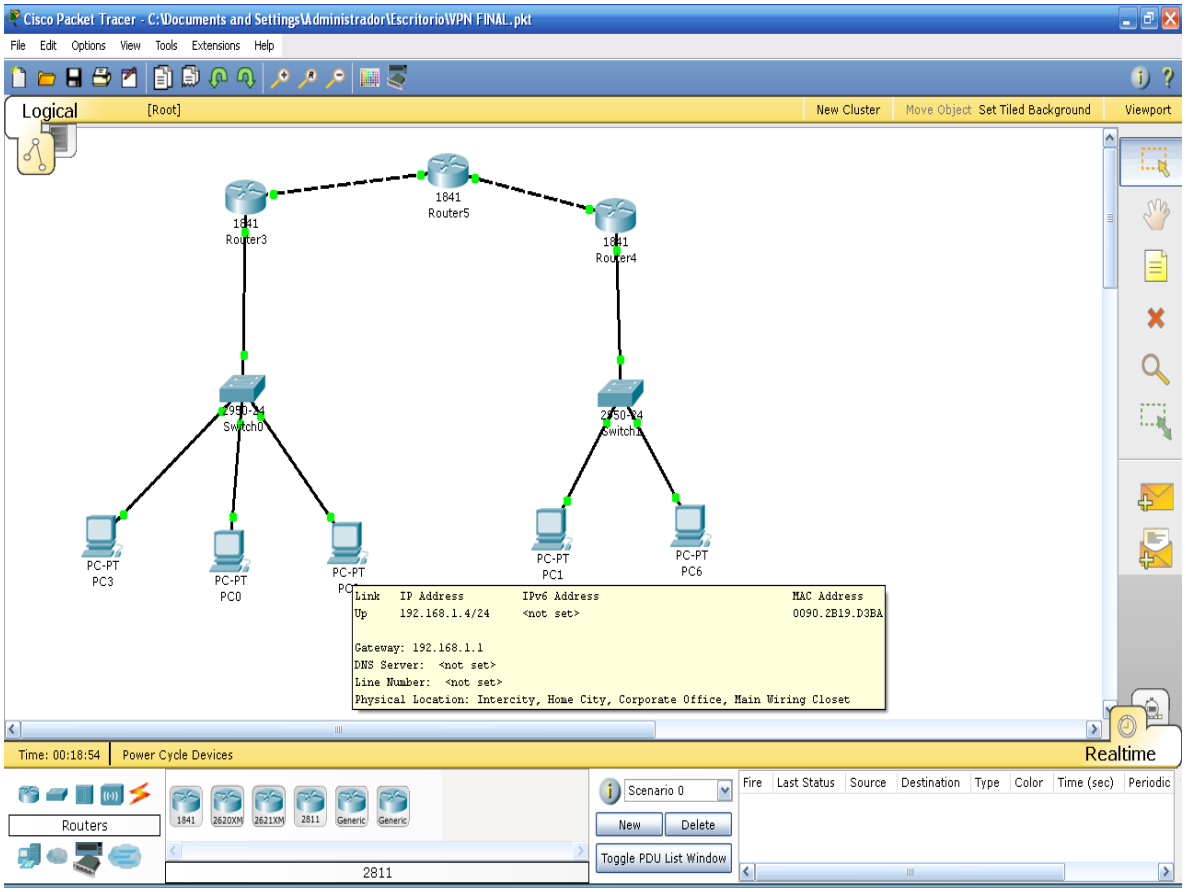
PC 0

En el PC0 de la parte LAN Router 3 se configura el Gateway 192.168.1.1 y la ip address 192.168.1.3 con una mascara de red 24: 255.255.255.0



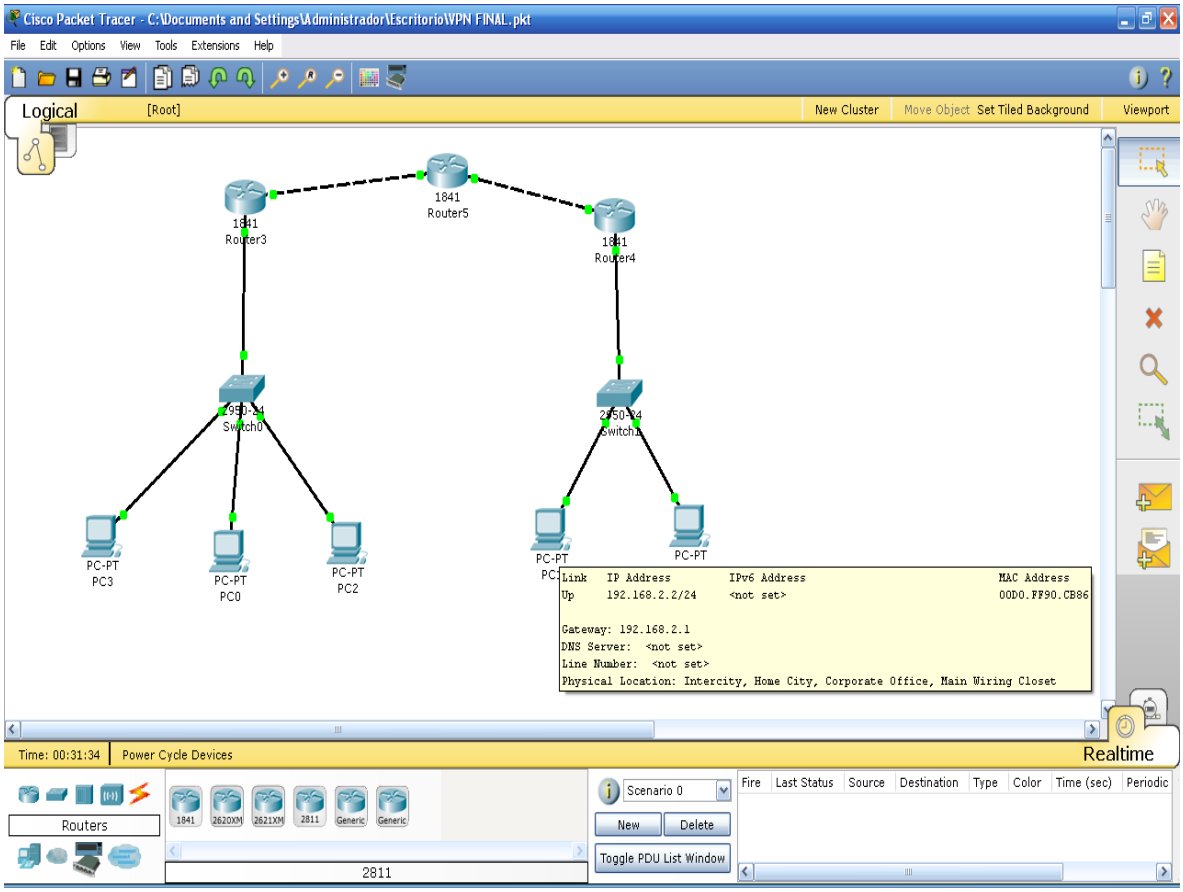
PC 2

En el PC2 de la parte LAN Router 3 se configura el Gateway 192.168.1.1 y la ip address 192.168.1.4 con una mascara de red 24: 255.255.255.0



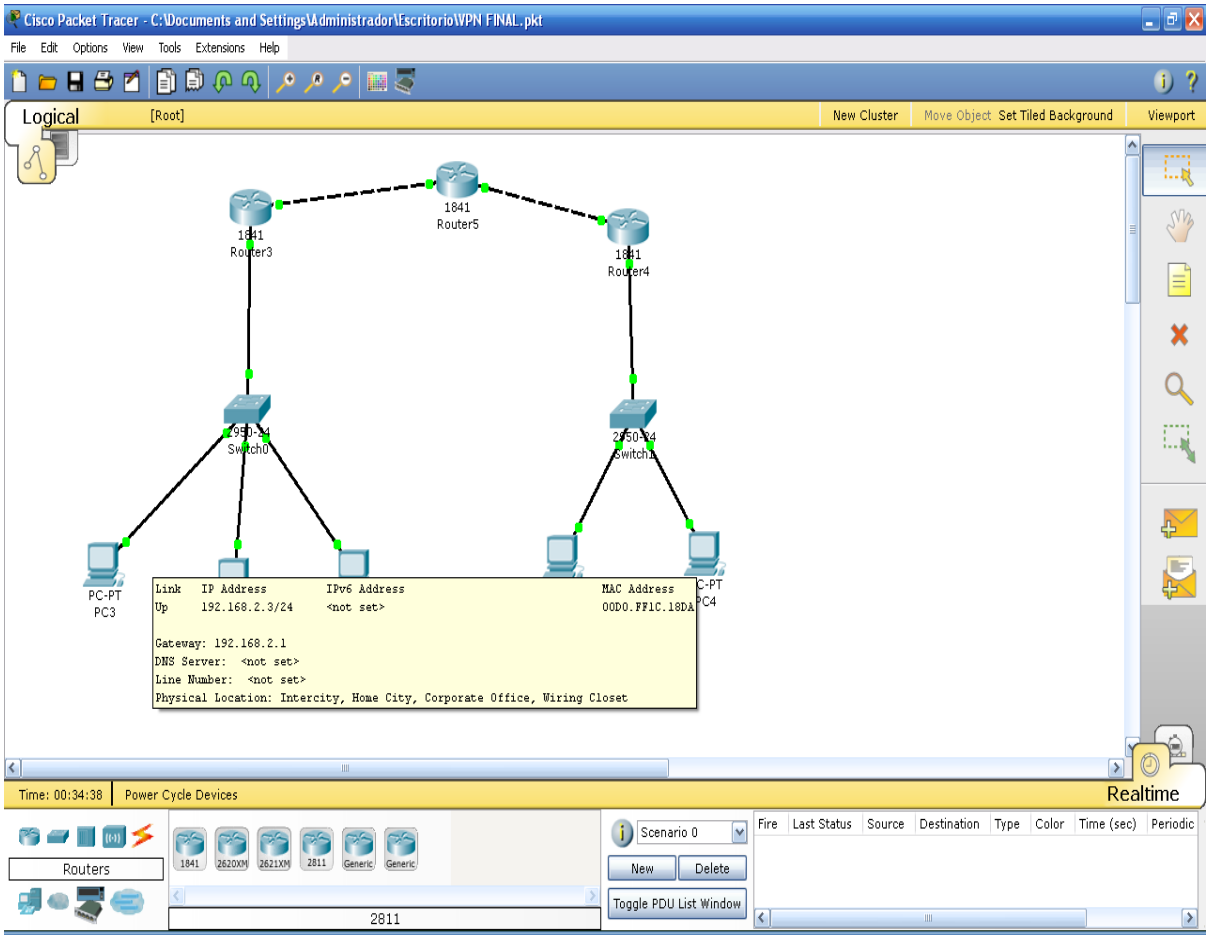
PC 1

En el PC1 de la parte LAN Router 4 se configura el Gateway 192.168.1.1 y la ip address 192.168.1.4 con una mascara de red 24: 255.255.255.0



PC 4

En el PC4 de la parte LAN Router 3 se configura el Gateway 192.168.1.1 y la ip address 192.168.1.4 con una mascara de red 24: 255.255.255.0

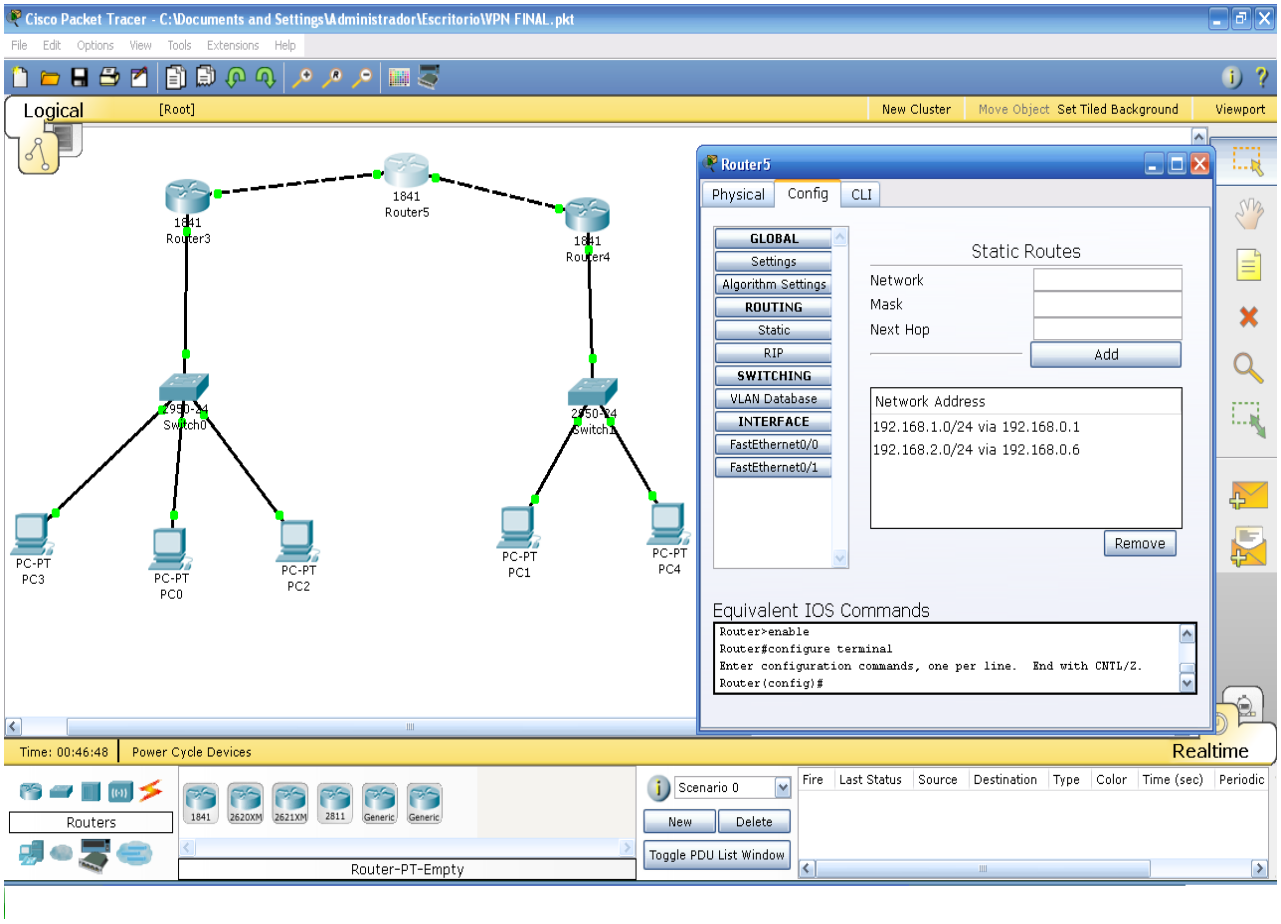


Router 5

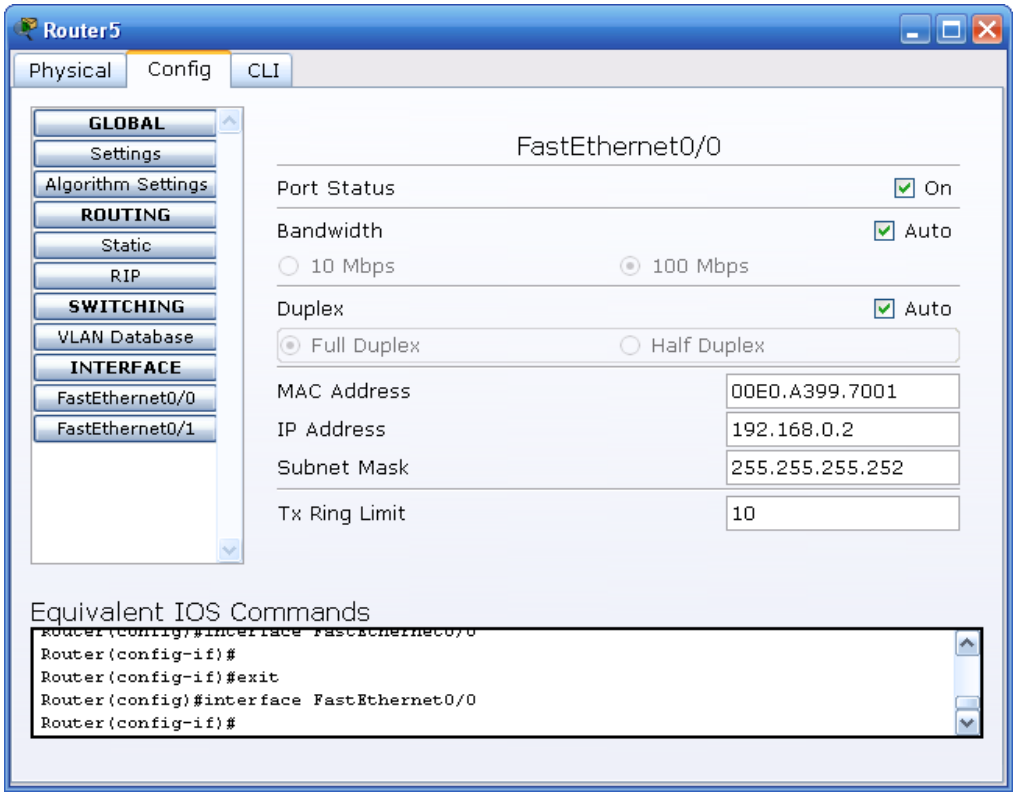
Se configura el router 5 especificando el enrutamiento estático:

192.168.1.0: que corresponde a una ip libre de la LAN del Router3 con un next hop o siguiente salto: 192.168.0.1 que corresponde a la WAN del Router 3

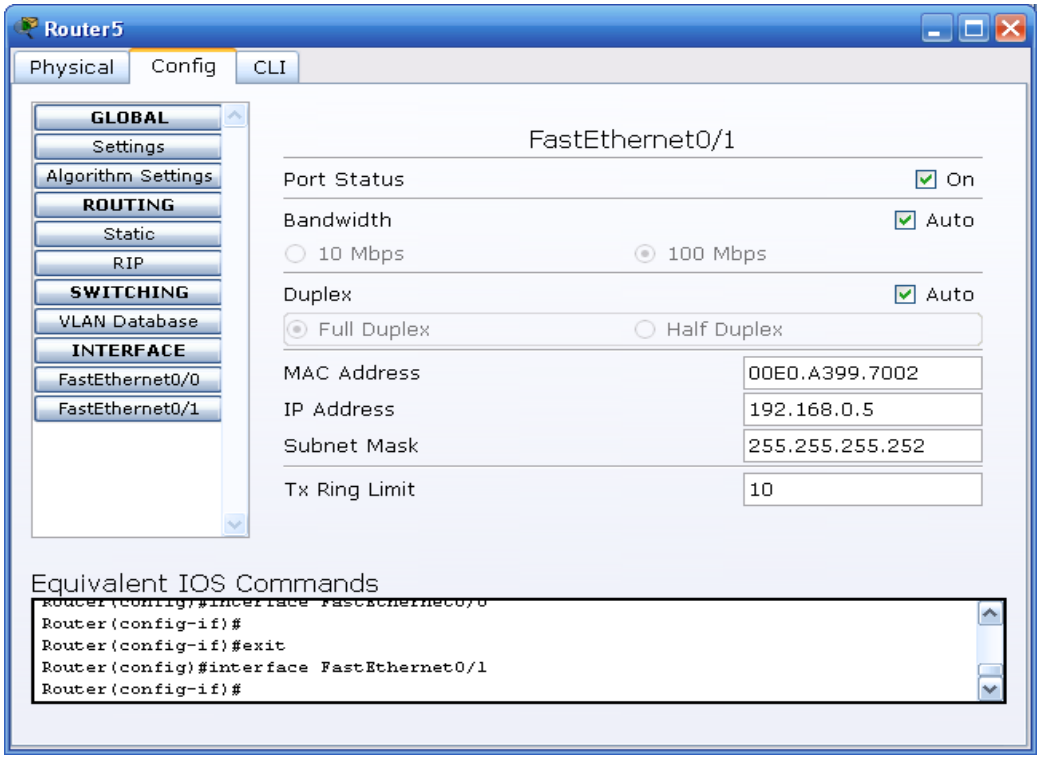
192.168.2.0: que corresponde a una ip libre de la LAN del Router4 con un next hop o siguiente salto: 192.168.0.6 que corresponde a la WAN del Router 3



Se configura la interface FastEthernet 0/0 con la ip libre 192.168.0.2 mascara de red 30 que es la próxima de la WAN (FastEthernet 0/1) del Router 3:



Se configura la interface FastEthernet 0/1 con la ip libre 192.168.0.5 mascara de red 30 que es la próxima de la WAN (FastEthernet 0/1) del Router 4:



VPN - ENCRIPTACION

Luego que se ha configurado los equipos y verificando que los paquetes lleguen a su destino solicitado, se realiza la encriptación de los paquetes para que Router 3 y Router 4 tengan una integridad y confidencialidad de toda la comunicación sin que Internet (Router 5) conozca el contenido de dichos paquetes:

En Router 3:

// En esta primera fase se realiza la configuración de intercambio de claves. Este proceso usa ISAKMP para identificar el algoritmo de hash y el método de autenticación. También se identifica uno de los extremos del túnel:

```
crypto isakmp policy 10     //

hash md5

 authentication pre-share     //  utilizará la clave definida más adelante

crypto isakmp key P5NM address 192.168.0.6   //  Se identifica la llave con la que
                                                 se va a encriptar los datos

no crypto isakmp ccm     //

!
```

// A continuación, creamos un IPsec conjunto de transformación que llamamos TRANSFORM. Se especifica el protocolo de encriptación IPsec para la carga de seguridad encapsuladora (ESP). Estos no tienen por qué ser la misma que protocols IKE utiliza.

```
crypto ipsec transform-set TRANSFORM esp-3des esp-md5-hmac //

 mode transport     //

crypto ipsec df-bit clear    //

!

crypto map QPDG00 10 ipsec-isakmp    //

 set peer 192.168.0.6     // extremo del tunel

 set transform-set TRANSFORM      //  cual set de transformación de paquetes
                                      utilizará

 match address 101      // origen-destino de paquetes

access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
//WILLCARD
```

interface FastEthernet0/1 //

crypto map QPDG00 //

En Router 4:

// En esta primera fase se realiza la configuración de intercambio de claves. Este proceso usa ISAKMP para identificar el algoritmo de hash y el método de autenticación. También se identifica uno de los extremos del túnel:

crypto isakmp policy 10

hash md5

authentication pre-share

crypto isakmp key P5NM address 192.168.0.1

no crypto isakmp ccm

!

// A continuación, creamos un IPsec conjunto de transformación que llamamos TRANSFORM. Se especifica el protocolo de encriptación IPsec para la carga de seguridad encapsuladora (ESP). Estos no tienen por qué ser la misma que protocols IKE utiliza.

crypto ipsec transform-set TRANSFORM esp-3des esp-md5-hmac

mode transport

crypto ipsec df-bit clear

!

crypto map QPDG00 10 ipsec-isakmp

set peer 192.168.0.1

set transform-set TRANSFORM

match address 101

access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

interface FastEthernet0/1

crypto map QPDG00

GLOSARIO

IPSec: Internet Protocol Security (IPSec) es un conjunto de protocolos que se utilizan para proteger las comunicaciones IP. IPSec incluye tanto intercambio de claves y el cifrado del túnel. Usted puede pensar en IPSec como un marco para la aplicación de la seguridad. Al crear una VPN IPSec, puede elegir entre una variedad de tecnologías de seguridad para aplicar el túnel.

ISAKMP (IKE): Internet Security Association and Key Management Protocol (ISAKMP) proporciona un medio para la autenticación de los pares en una comunicación segura. Suele utilizar Internet Key Exchange (IKE), pero otras tecnologías también pueden ser utilizados. Las claves públicas o una clave previamente compartida se utiliza para autenticar las partes en la comunicación.

MD5: Message-algoritmo Digest 5 (MD5) es un uso frecuente, pero en parte la inseguridad función de hash criptográfica con un valor de hash de 128-bits. Una función de hash criptográfica es una manera de tomar una de bloques de datos y el retorno de una determinada cadena de bits de tamaño, el valor hash basado en el bloque original de datos. El proceso de dispersión se ha diseñado de modo que un cambio en los datos también cambiará el valor de hash. El valor hash es también llamado el resumen del mensaje.

SHA: Secure Hash Algorithm (SHA) es un conjunto de funciones de hash criptográfica diseñado por la Agencia de Seguridad Nacional (NSA). Los algoritmos SHA tres están estructuradas de manera diferente y se distinguen como SHA-0, SHA-1 y SHA-2. SHA-1 es un algoritmo de hash de uso común, con una longitud de clave de 160 bits estándar.

ESP: Carga de seguridad encapsuladora (ESP) es un miembro de la suite de protocolo IPsec que proporciona autenticidad de origen, la integridad,

confidencialidad y protección de los paquetes. ESP también soporta el cifrado y la autenticación de sólo-sólo configuraciones, pero utilizar cifrado sin autenticación está totalmente desaconsejado, ya que es inseguro. A diferencia del protocolo IPsec otros, Authentication Header (AH), ESP no protege a la cabecera del paquete IP. Esta diferencia hace ESP preferido para su uso en una configuración de traducción de direcciones de red. ESP opera directamente sobre IP, utilizando el protocolo IP número 50.

DES: El Data Encryption Standard (DES) proporciona encriptación de 56-bits. Ya no es considerado un protocolo seguro porque su clave de corta duración lo hace vulnerable a ataques de fuerza bruta.

3DES: Tres DES fue diseñado para superar las limitaciones y debilidades de DES usando tres diferentes claves de 56 bits en una operación de cifrar, descifrar, y volver a cifrar. 3DES claves de 168 bits de longitud. Cuando se utiliza 3DES, los datos es la primera cifra con una clave de 56 bits, a continuación, descifra con un 56 diferentes-bit, el resultado de que luego se vuelve a cifrar con un tercero 56-bit.

AES: El estándar de cifrado avanzado (AES), fue diseñado como un reemplazo para DES y 3DES. Está disponible en diferentes longitudes de clave y es considerado generalmente como unas seis veces más rápido que 3DES.

HMAC: El hashing Message Authentication Code (HMAC) es un tipo de código de autenticación de mensajes (MAC). HMAC se calcula mediante un algoritmo específica que incluya una función de hash criptográfica en combinación con una clave secreta