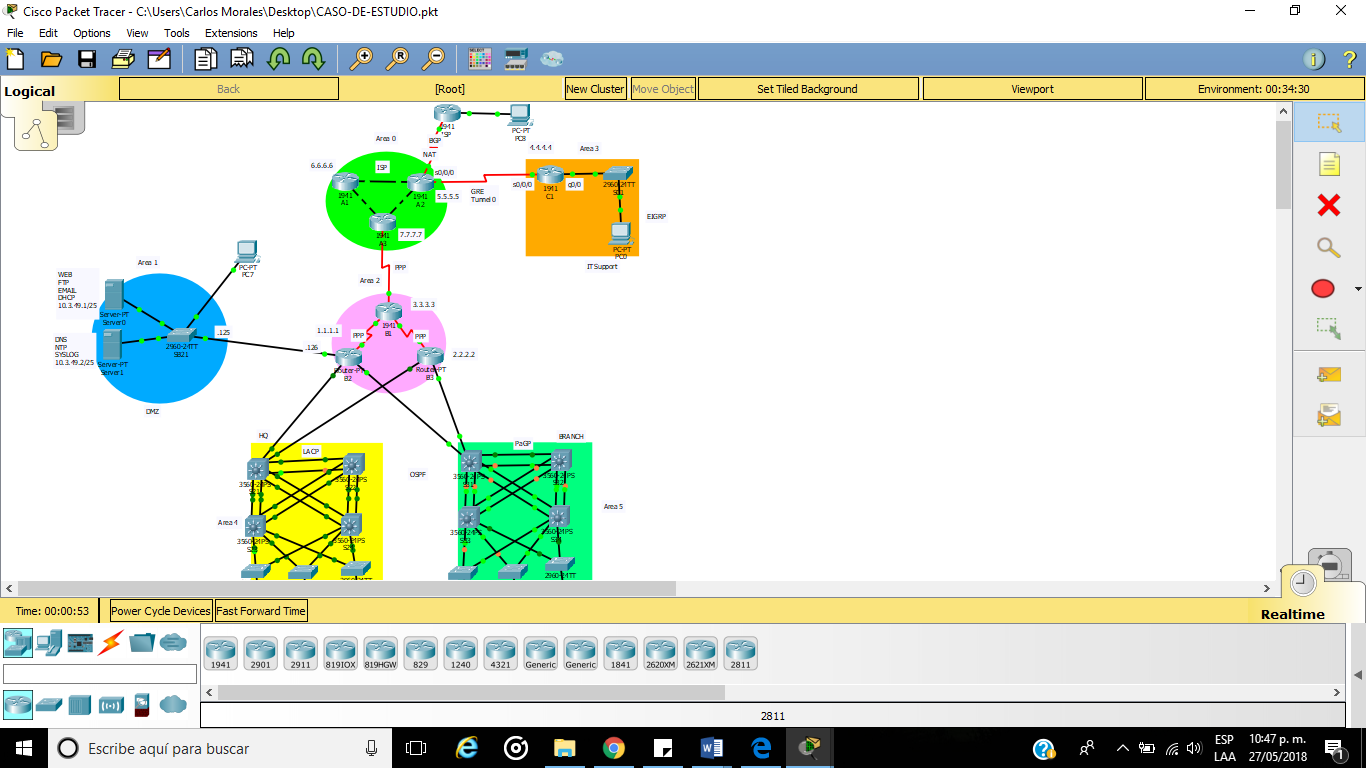
Paso 1 - Topología



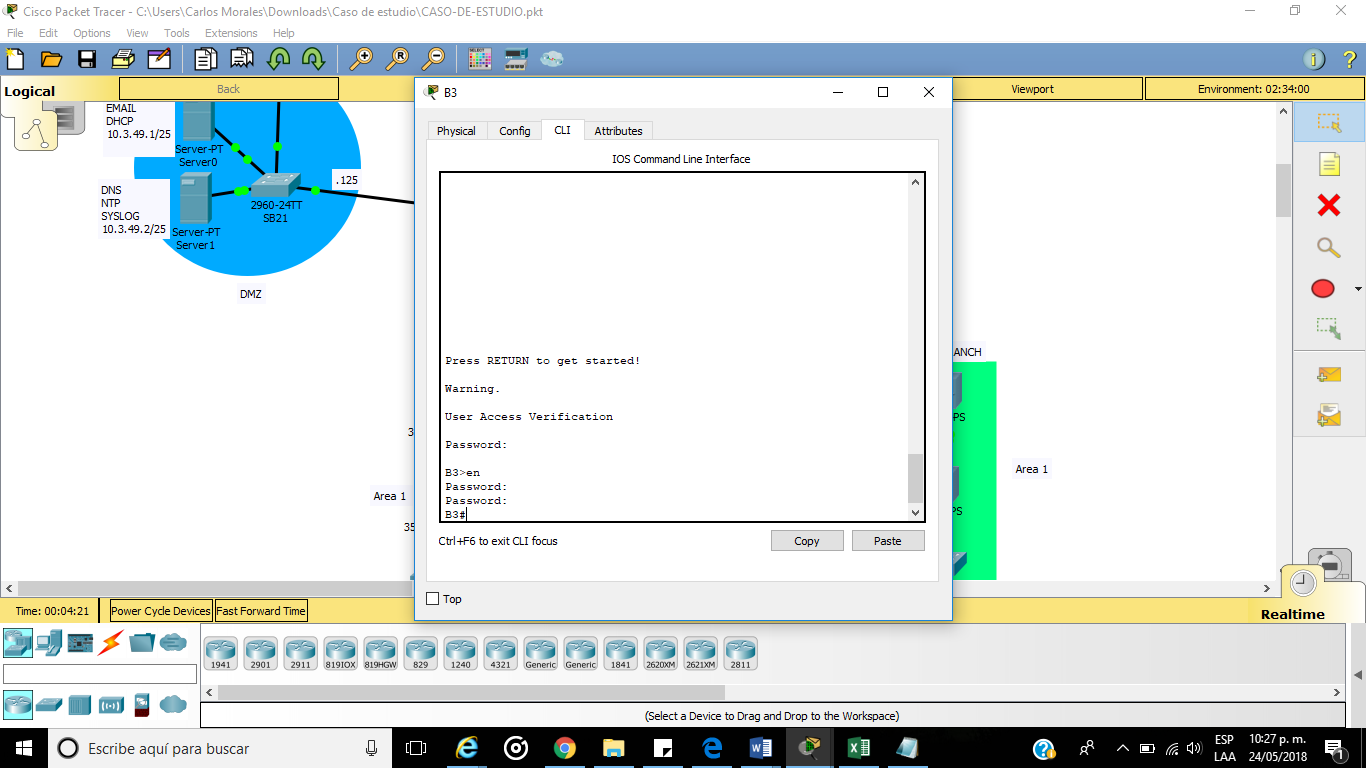
Paso 2 - Direccionamiento VLSM



Paso 3 – Configuración Básica

En todos los dispositivos (Switches y Routers) se ingresaron los siguientes comandos.

no ip domain-lookup

hostname -------

service password-encryption

enable secret class

banner motd #Warning.#

line con 0

password cisco

login

logging synchronous

line vty 0 4

password cisco

login

exit

ip domain-name cisco.com

crypto key generate rsa

1024

username admin secret cisco

line vty 0 4

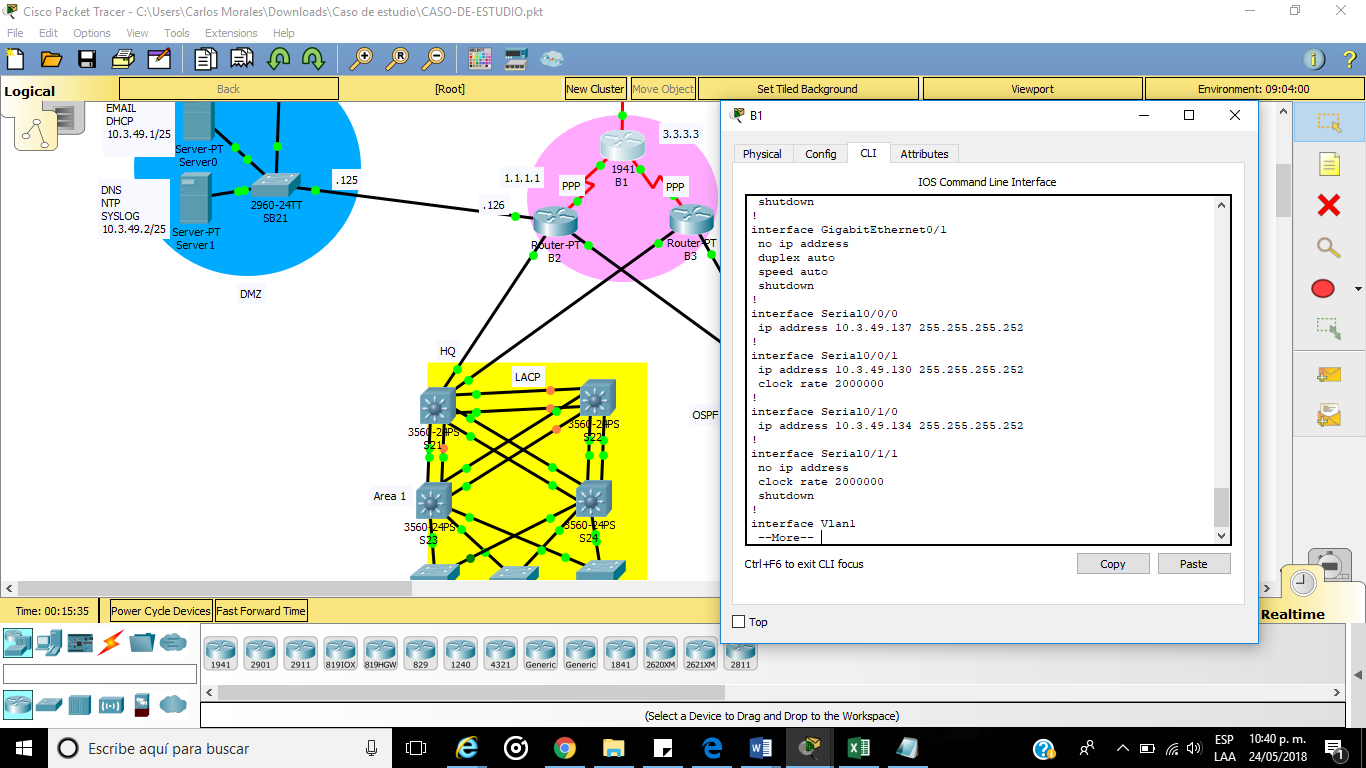
transport input ssh

login local

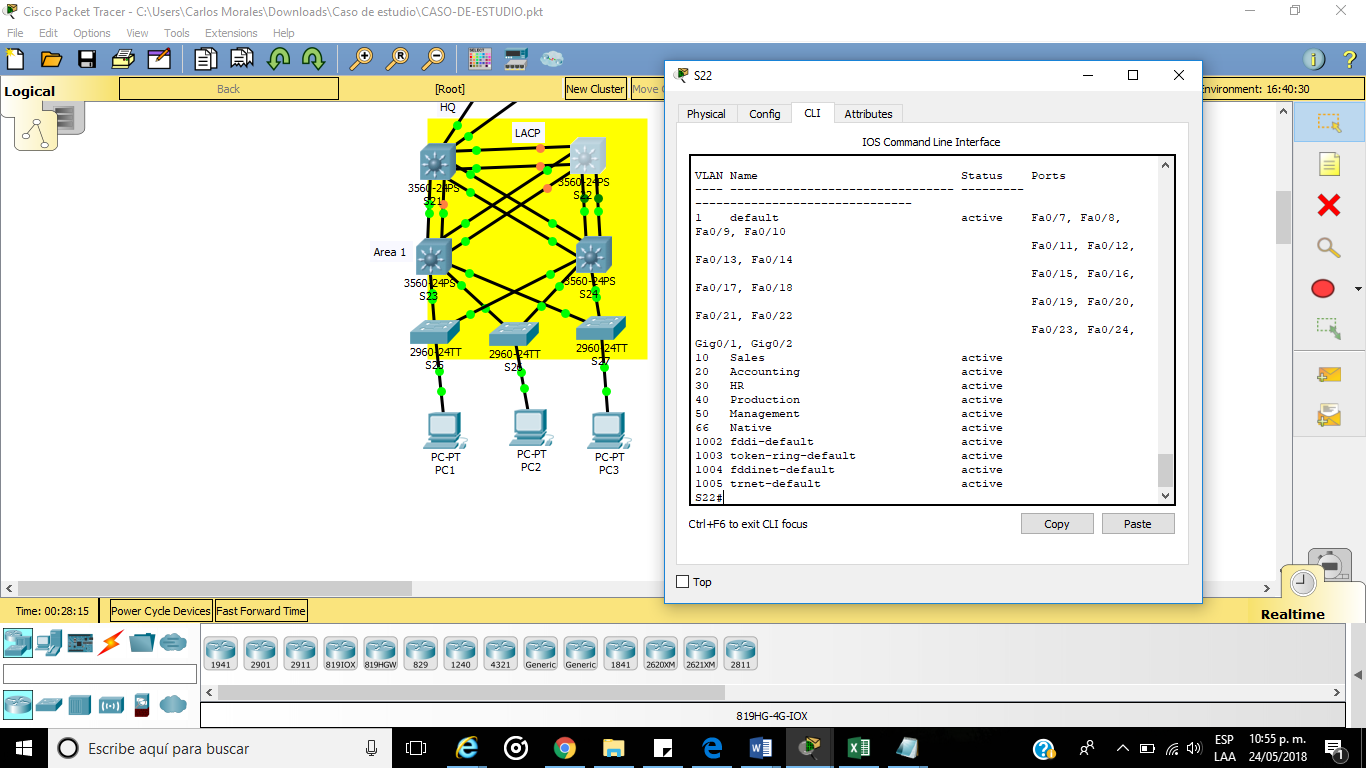
exit

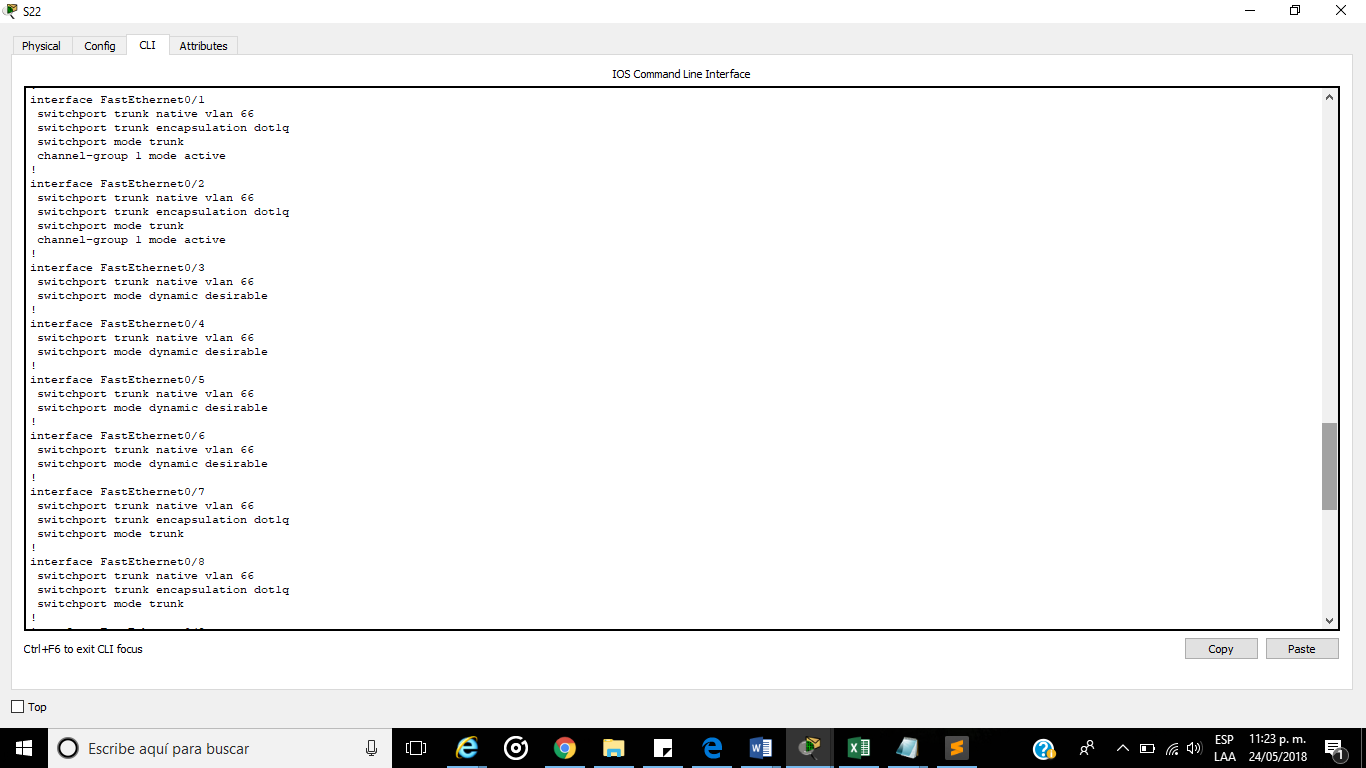
ip ssh version 2

Paso 4 – Configuración del direccionamiento en cada dispositivo de la topología. A continuación, se muestra la salida del comando show run en un router.

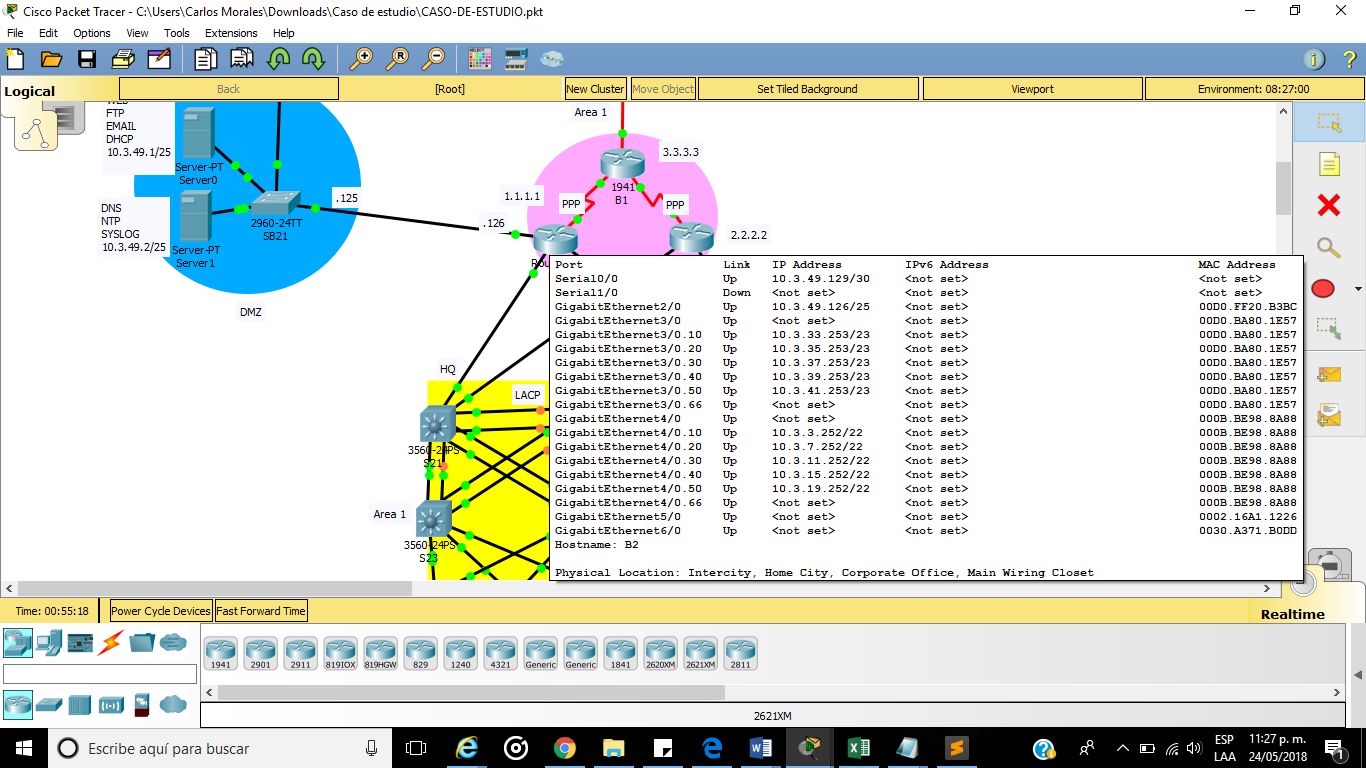


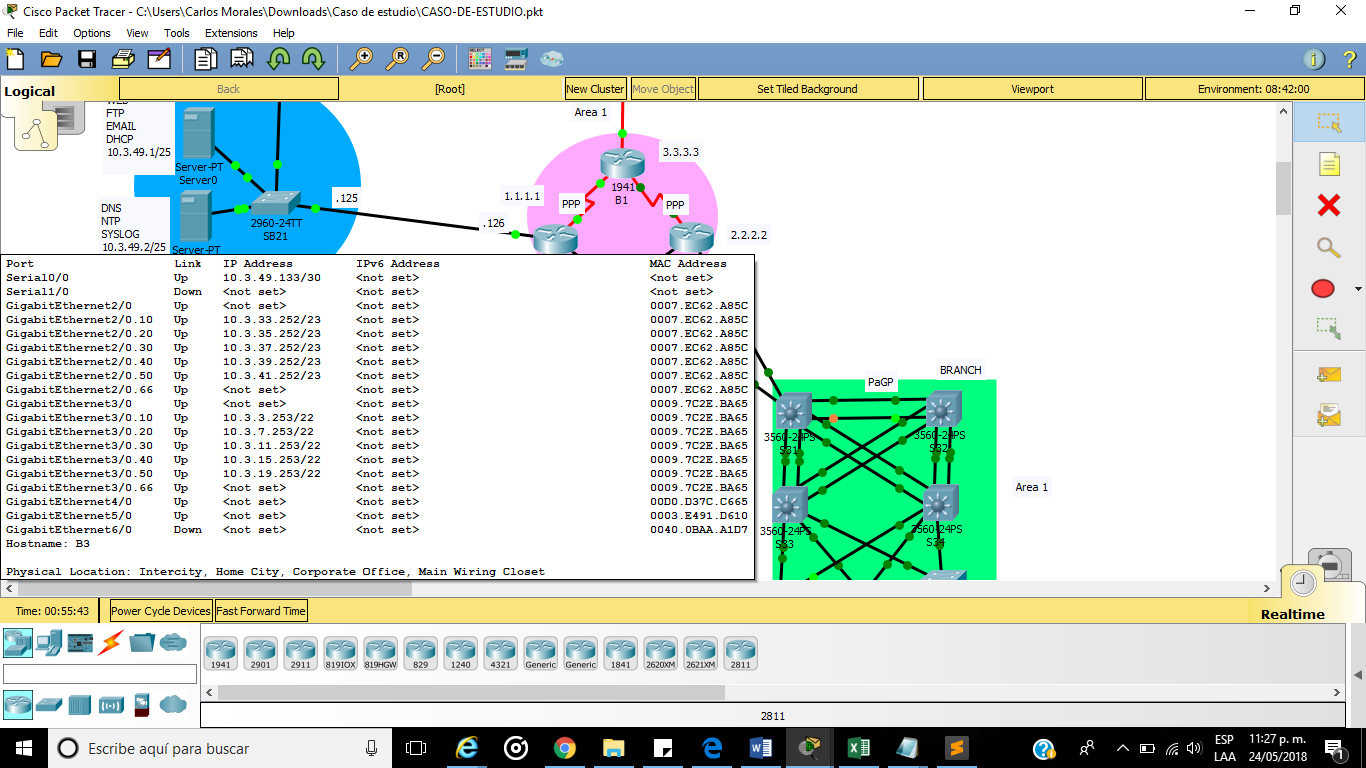
Paso 5 - Configuración de VLANS y Enlaces Troncales.



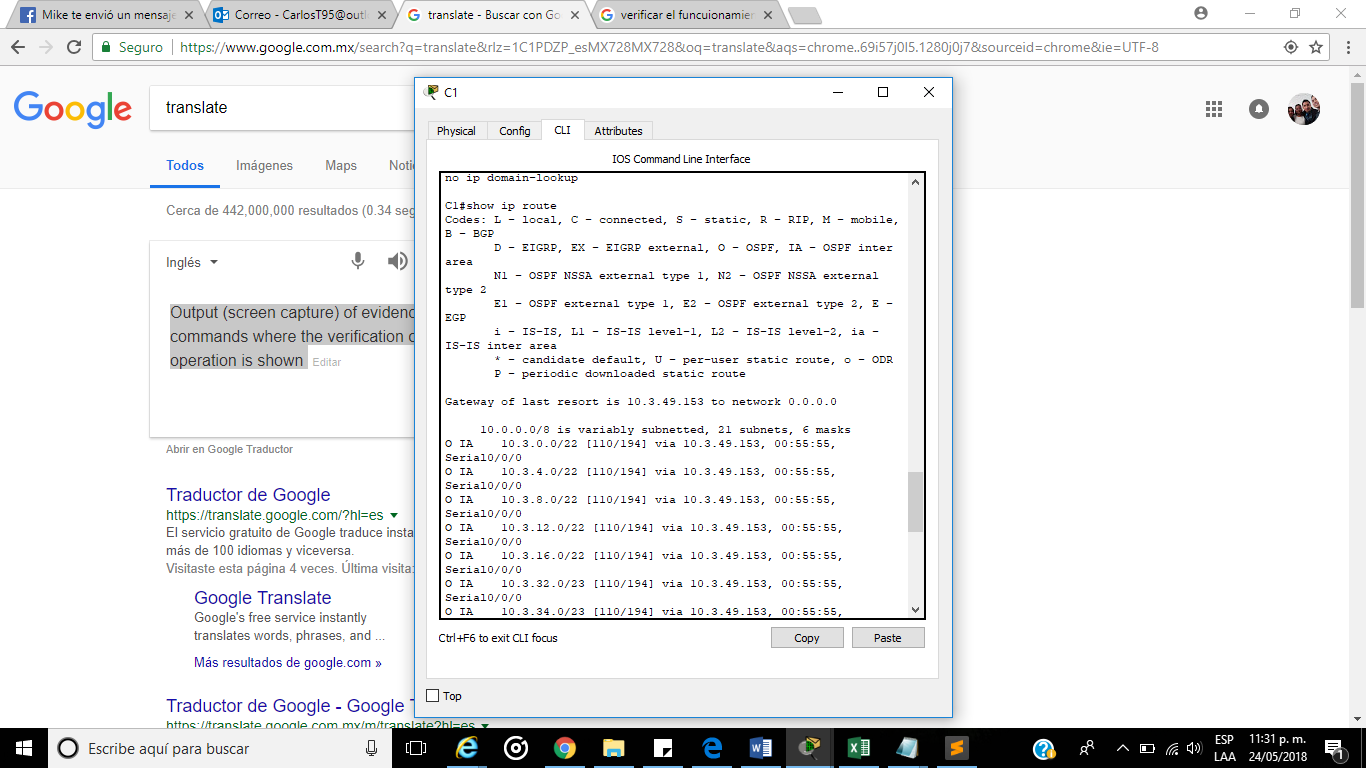


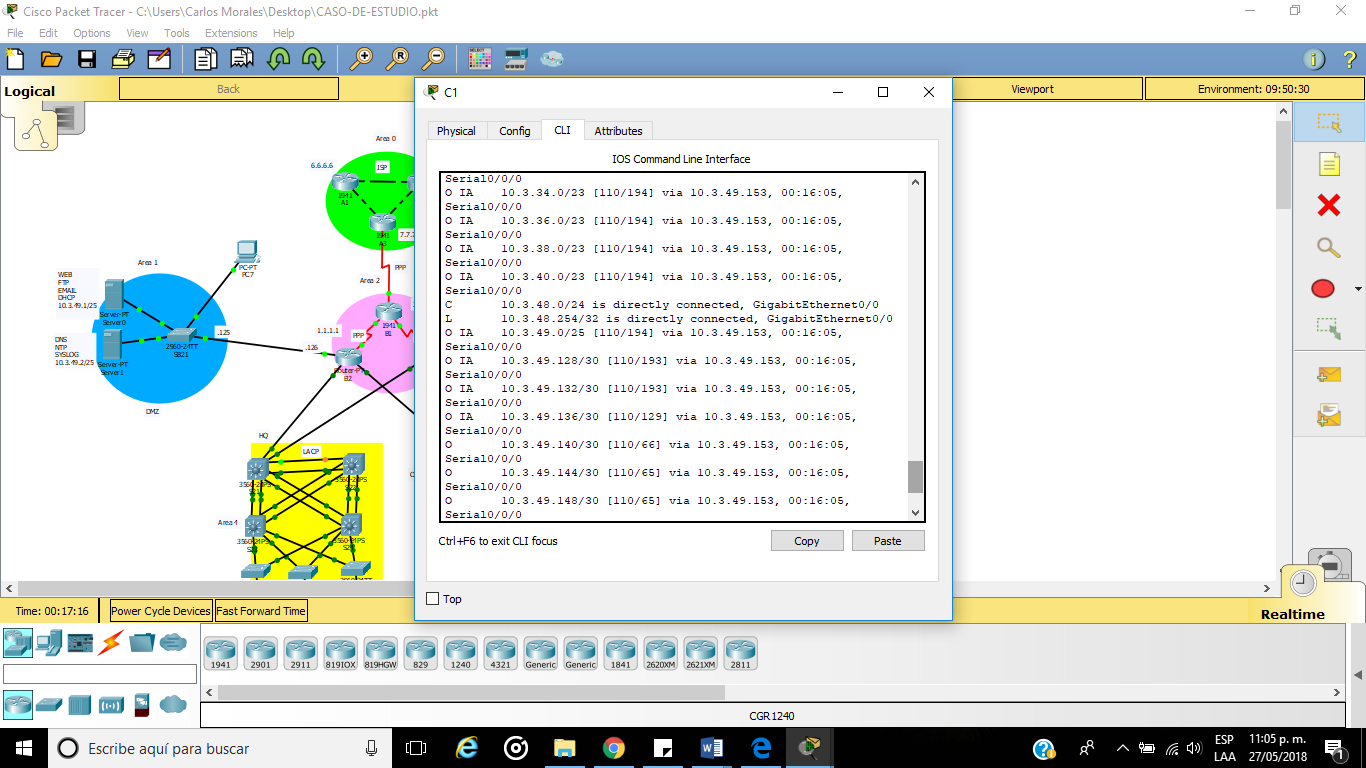
Paso 6 – Configuración Inter-Vlan.



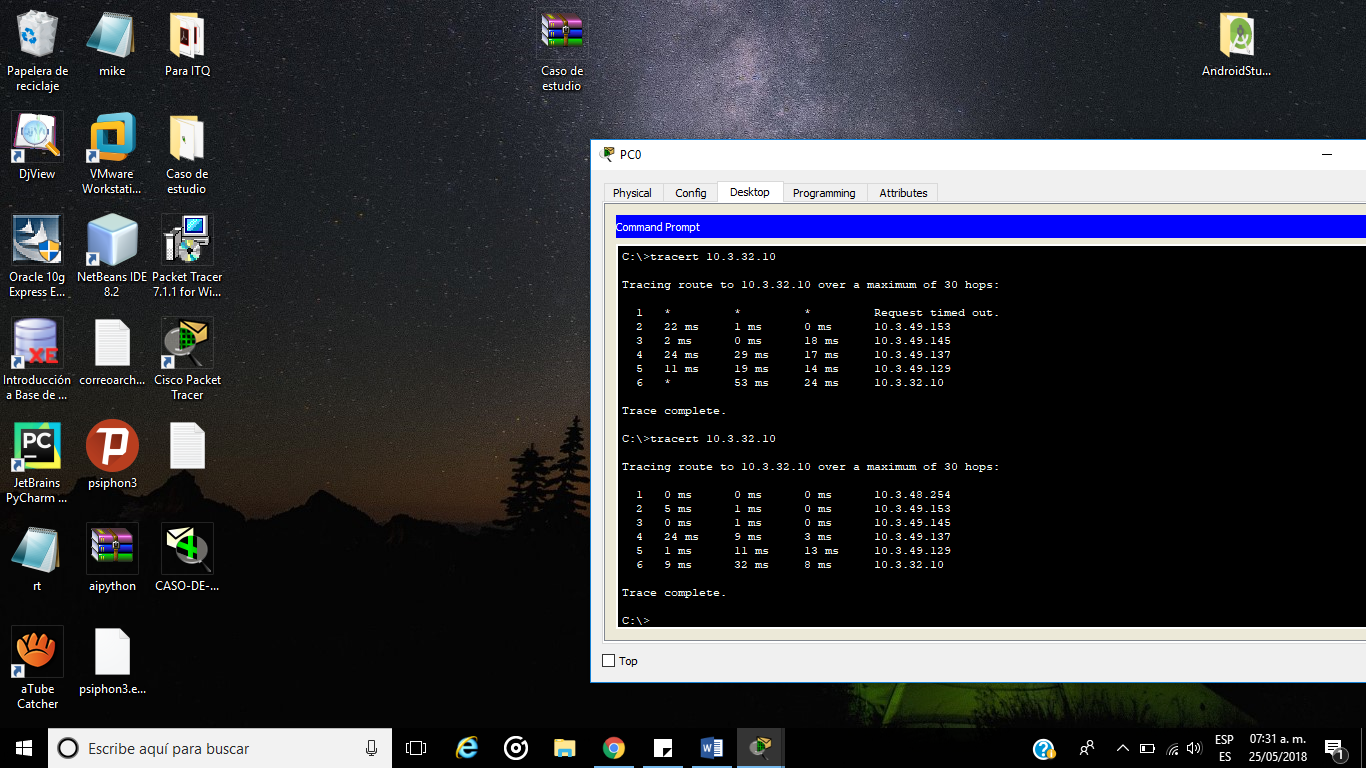


Paso 7 – Enrutamiento Dinámico OSPF multi área.

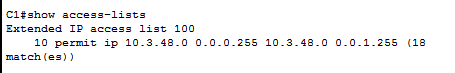
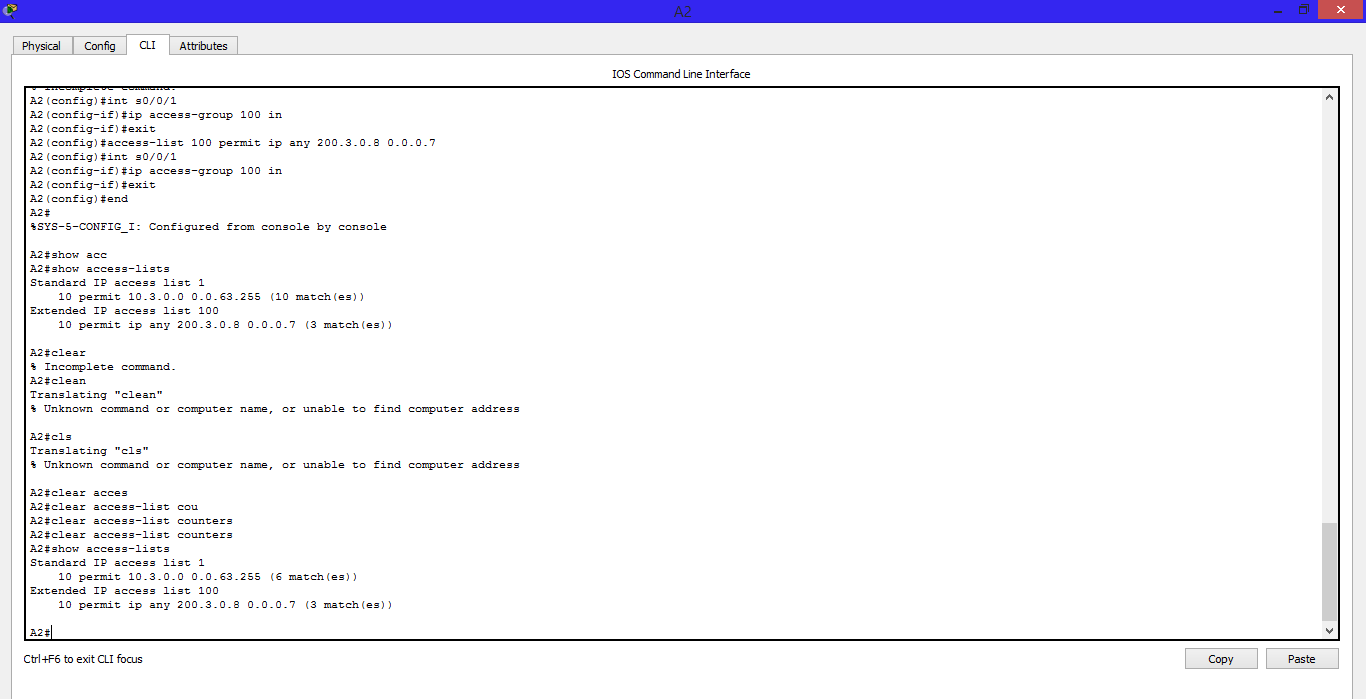




Tracert de un área 3 a la 5



Paso 8 – Configuración de ACLS estándar y extendidas



Como podemos ver las listas de acceso se configuraron en C1 y A2 y los comandos que se usaron para verificar su funcionalidad fueron show access-list, clear access-list counters, ping.

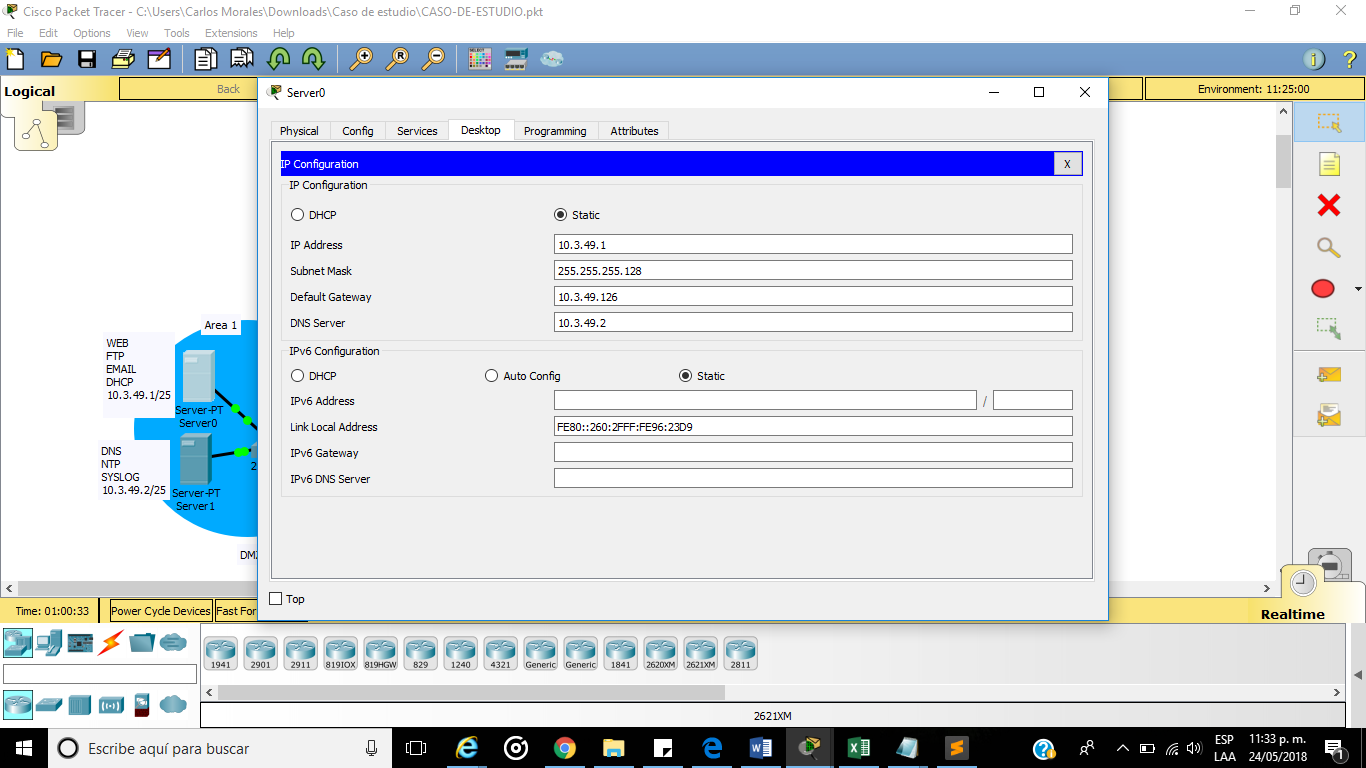
El comando show access-list nos sirve para verificar en el router las sentencias que se han cumplido de la lista de acceso.

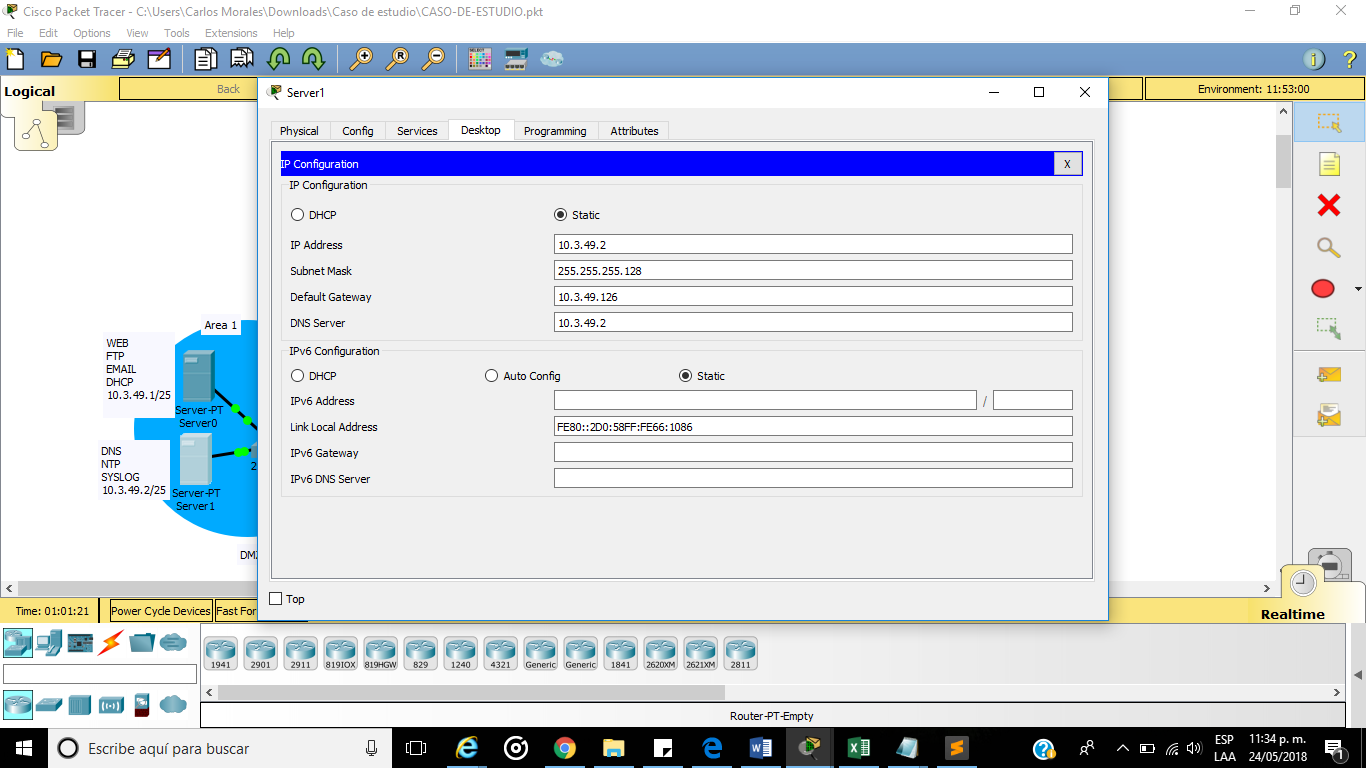
El comando clear access-list counters nos sirve para resetear los contadores, es muy util cuando se quiere probar el funcionamiento de una acl.

El comando ping nos sirve para llegar a una direccion de destino con el proposito de aumentar los contadores de la acl y es bueno usar este comando con show access-list.

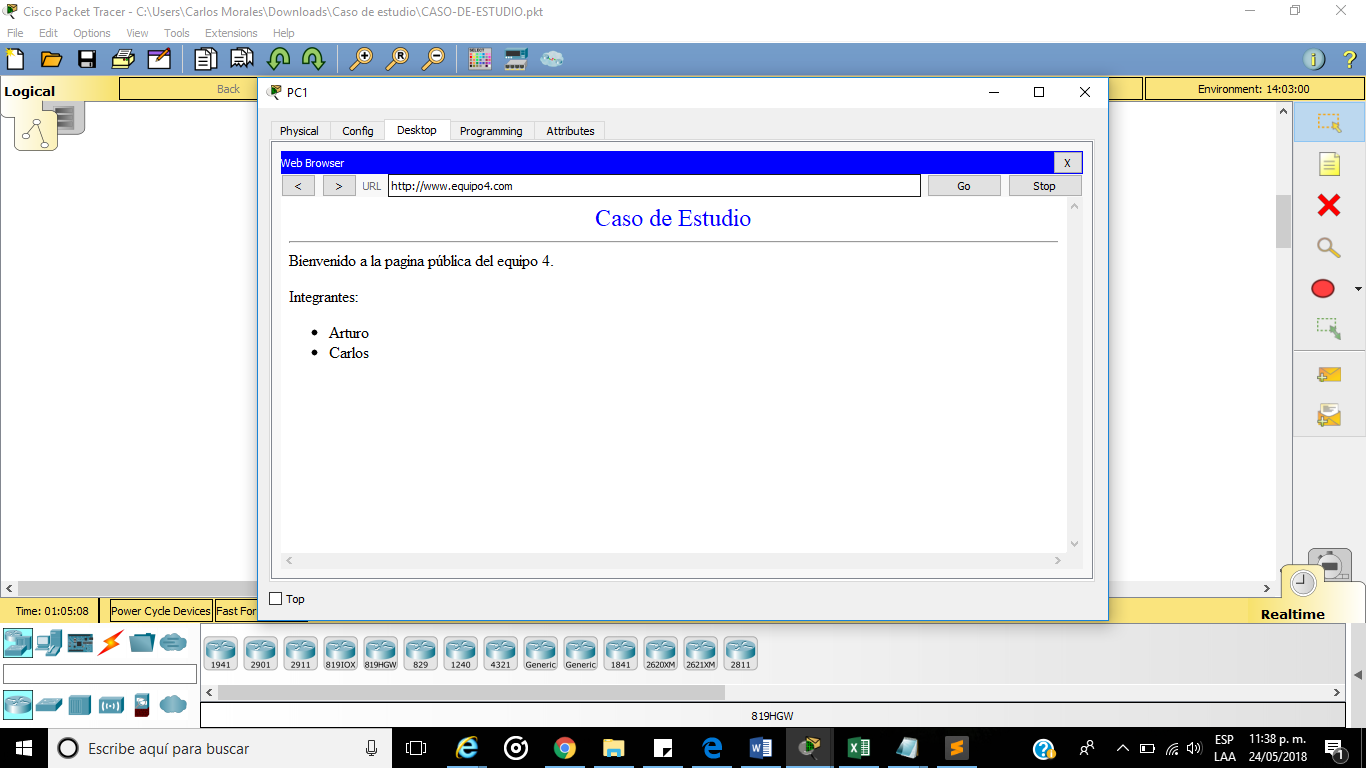
Paso 9 – Servidores.

Direcciones estáticas en los servidores

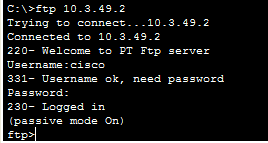




1. WEB

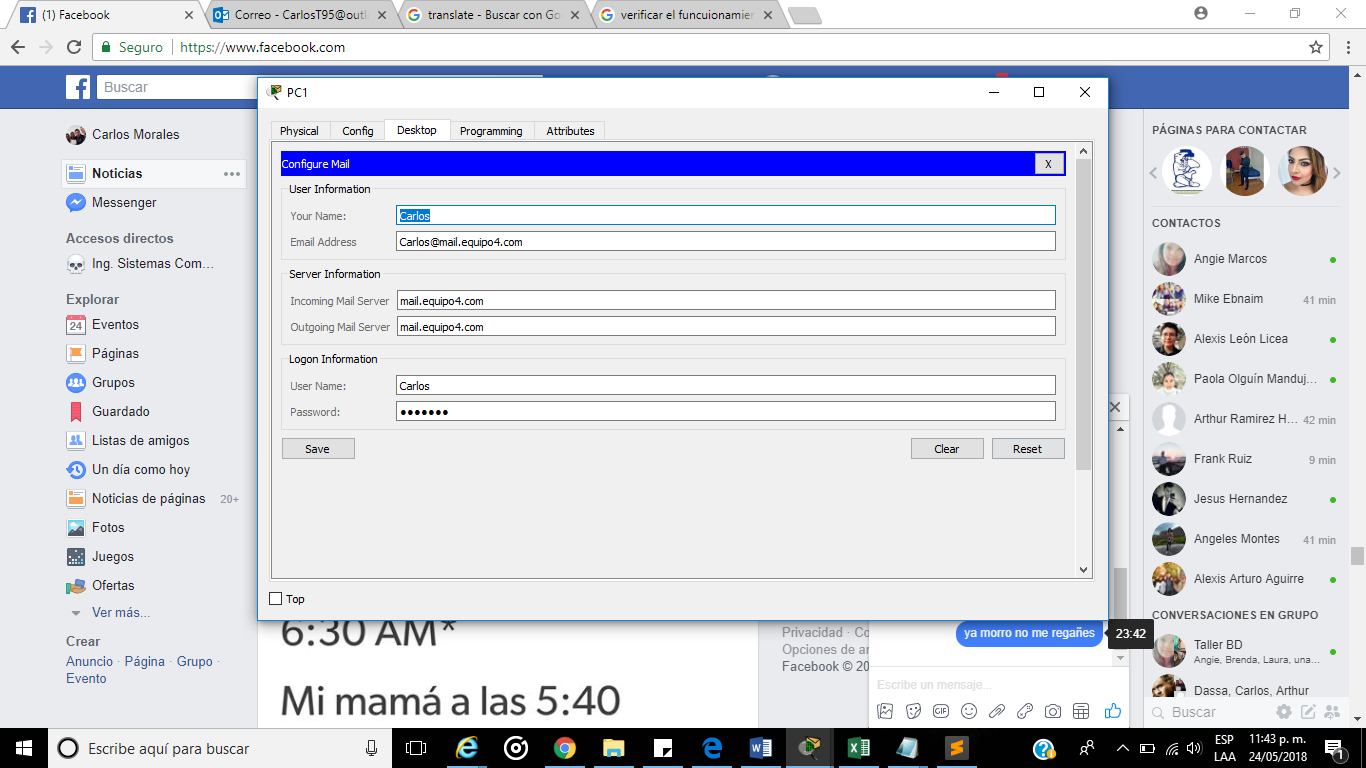


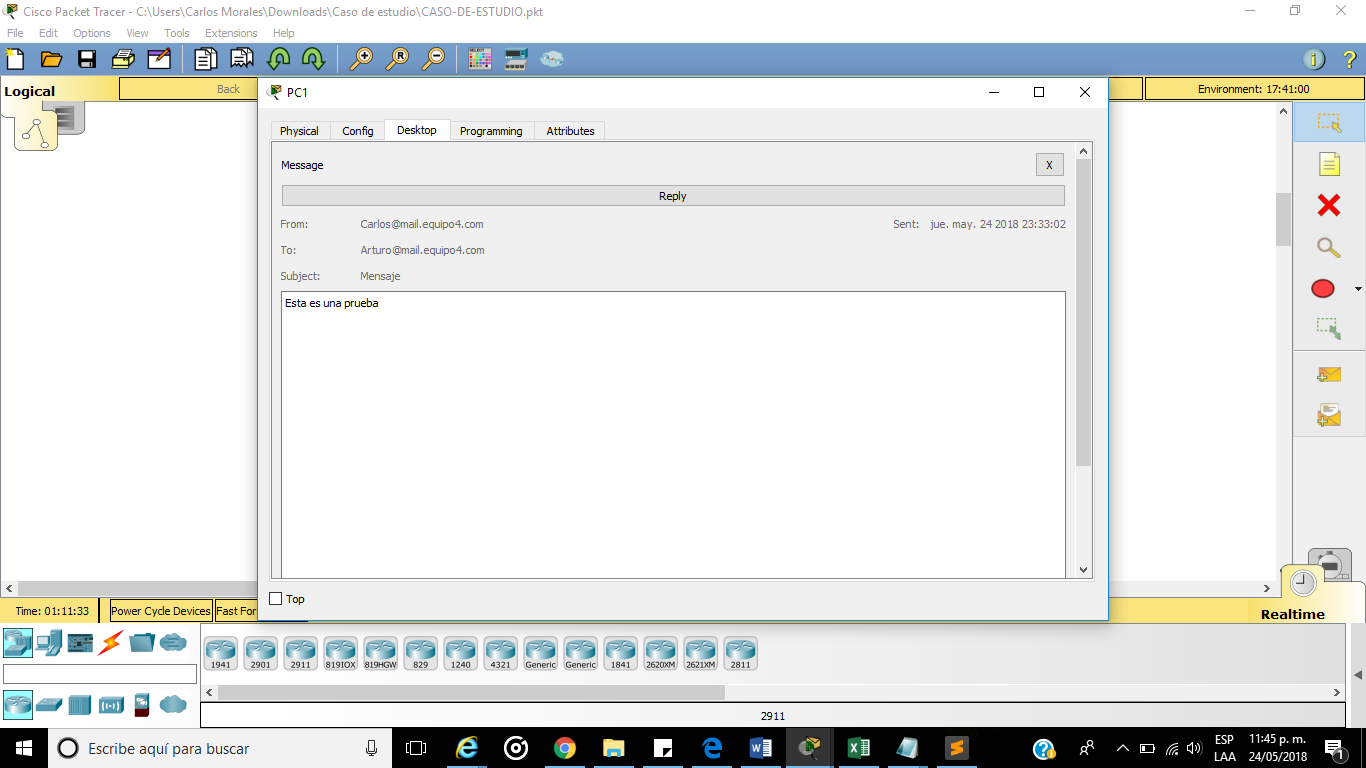
1. FTP



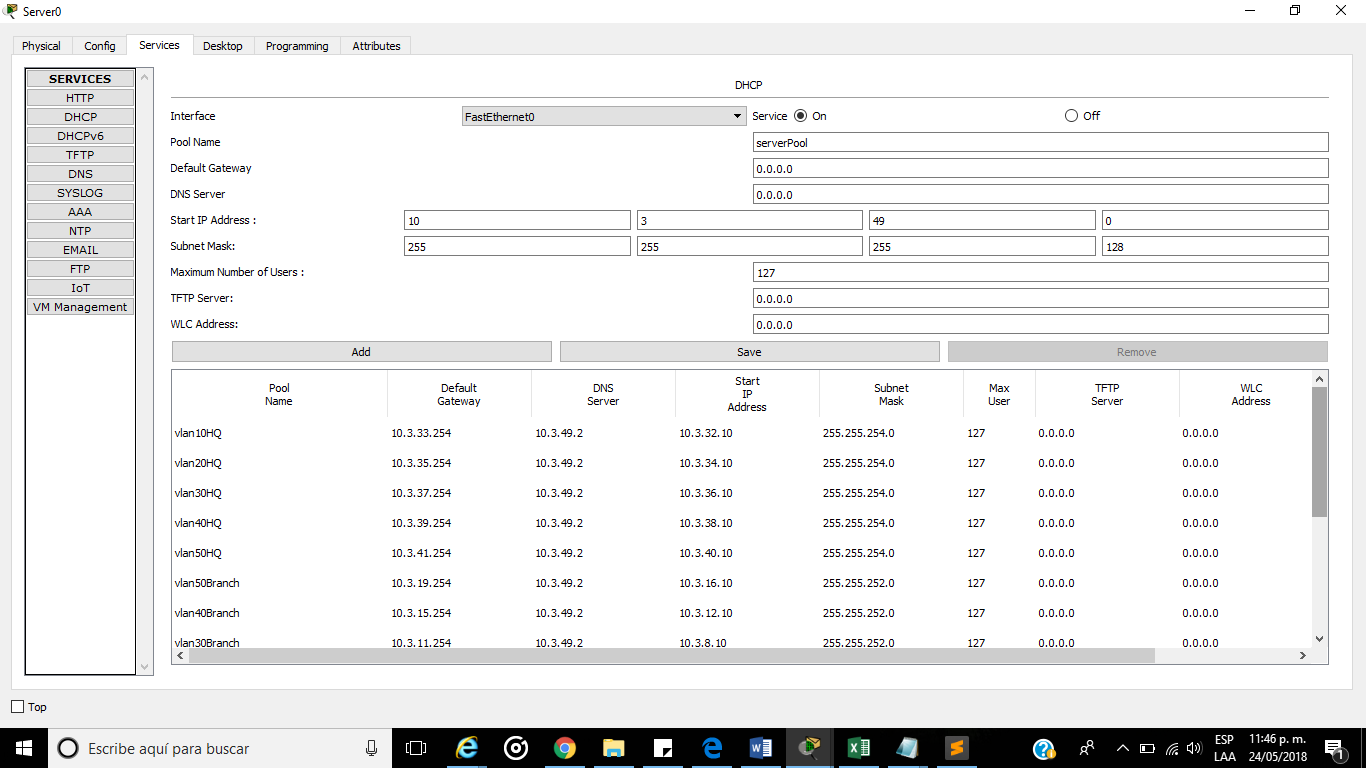
Cabe destacar que la ip ingresae en el comando ftp direccion\_ip es la direccion ip del servidor FTP.

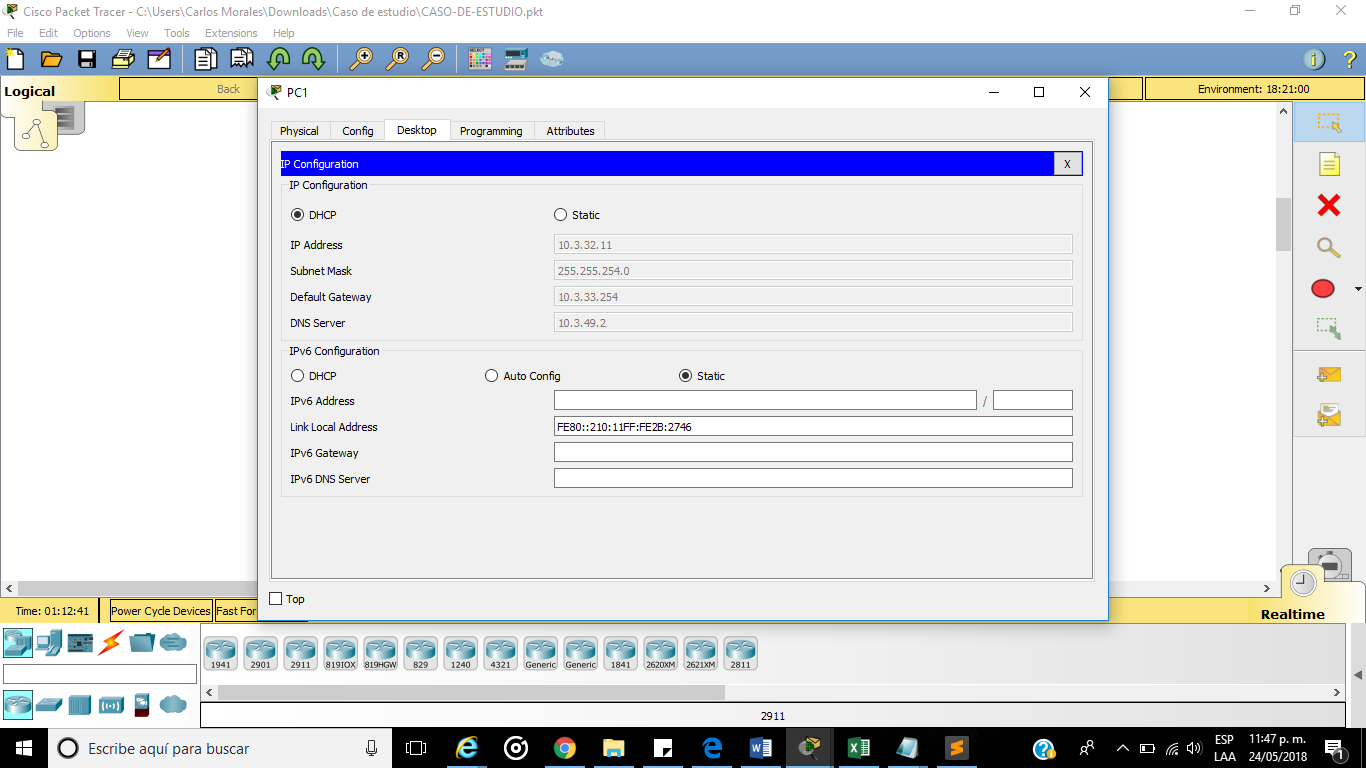
1. EMAIL





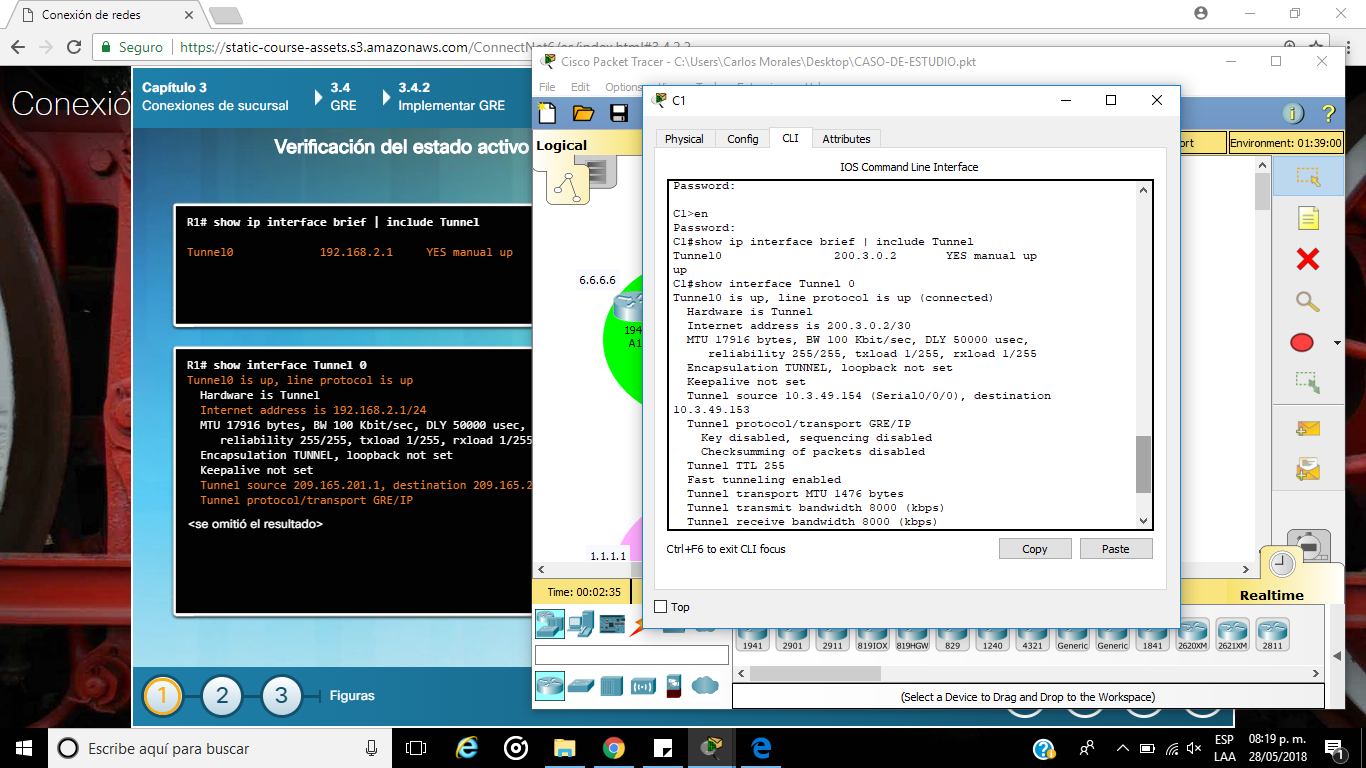
1. DHCP

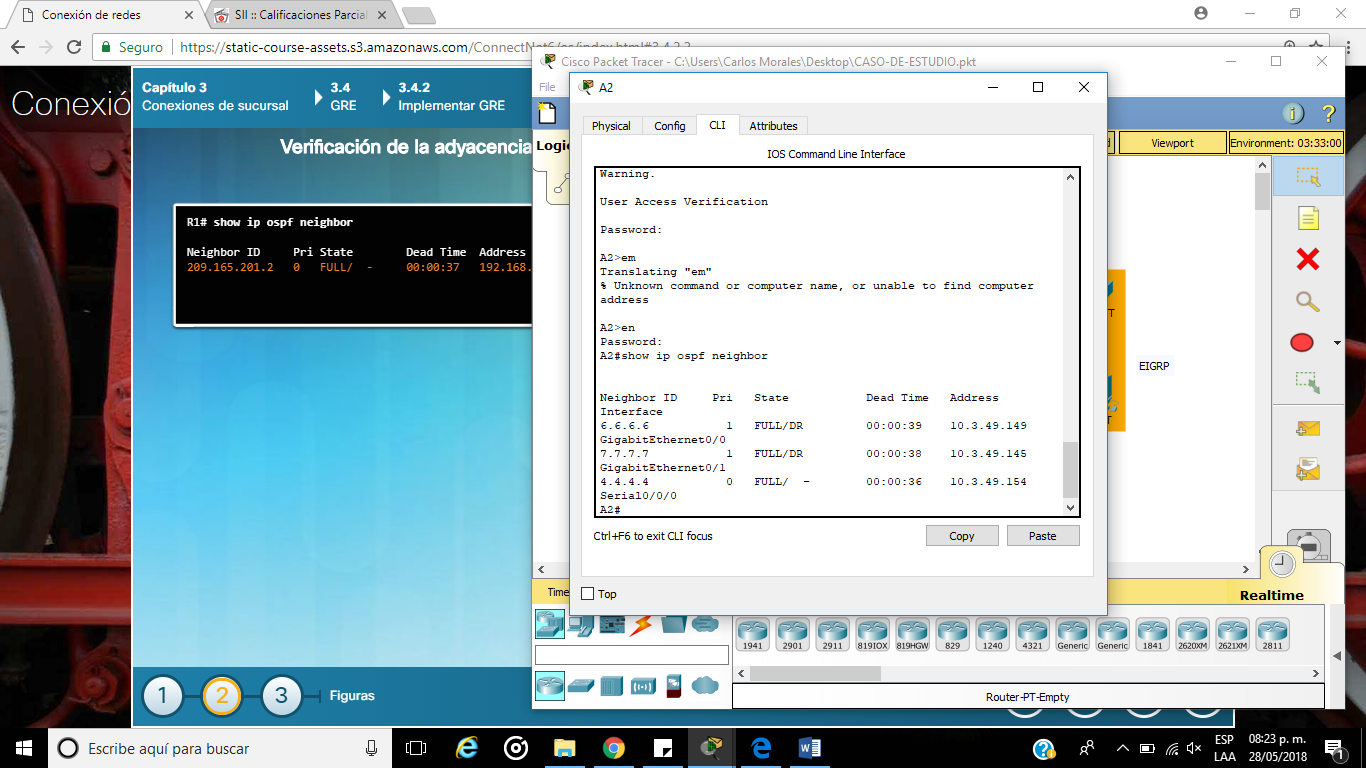


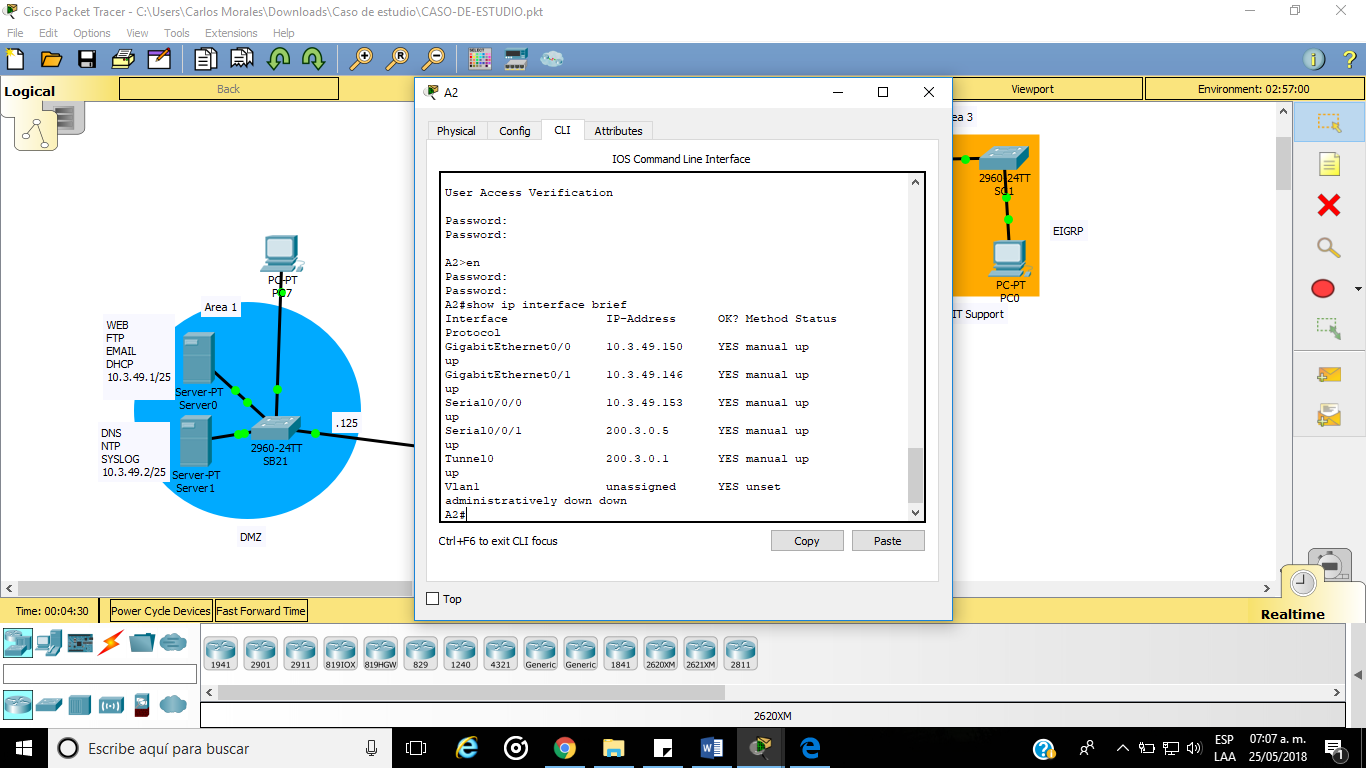


Paso 10 – Seguridad

GRE, VPN y Tunnel.



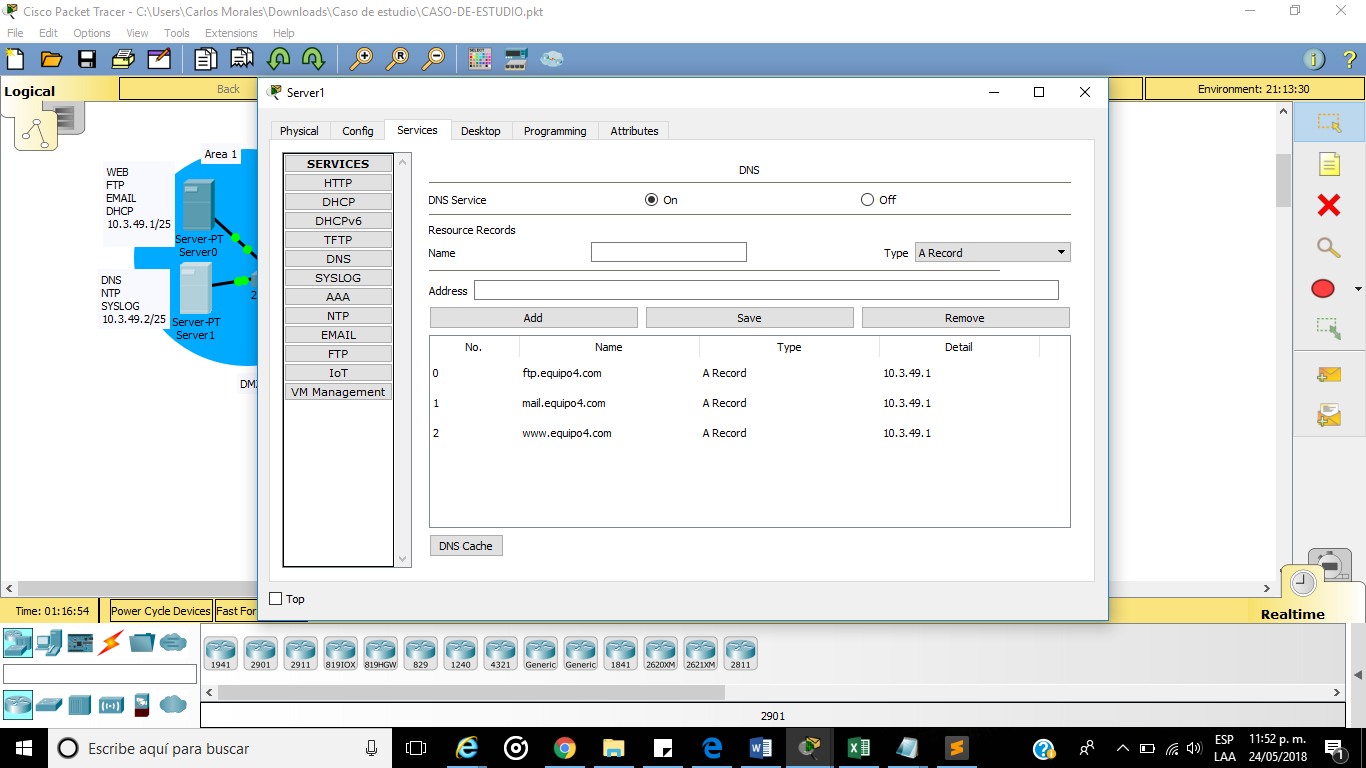




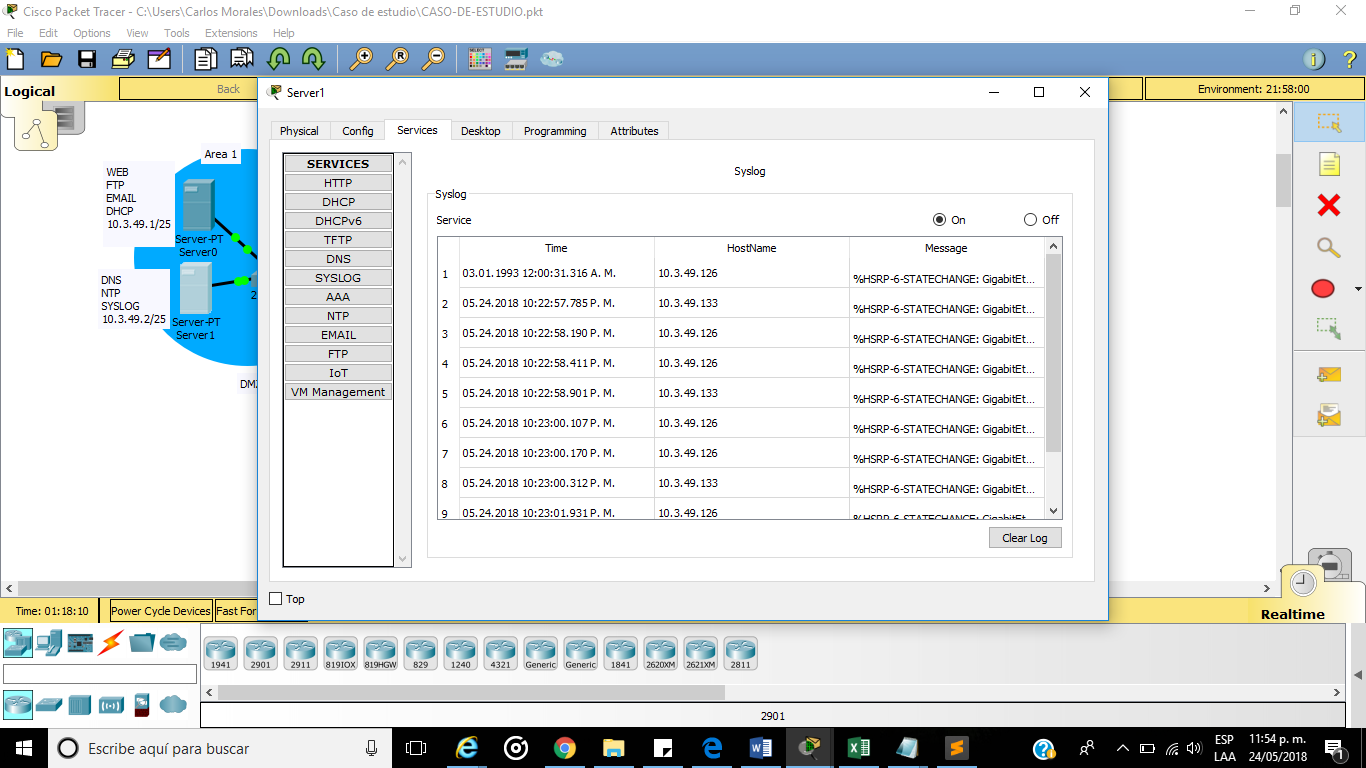
Paso 11 – Administración

Configuración de los siguientes servicios

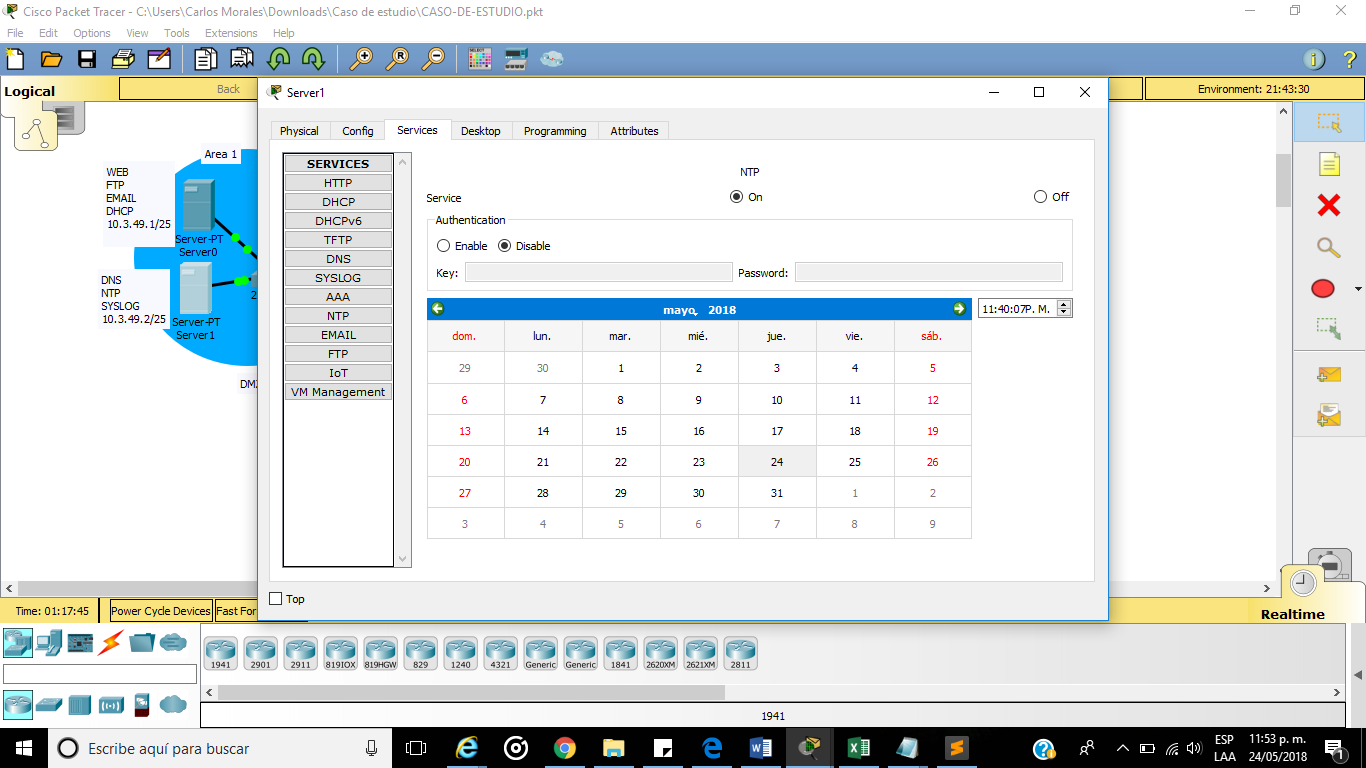
1. DNS



1. NAT
2. SYSLOG

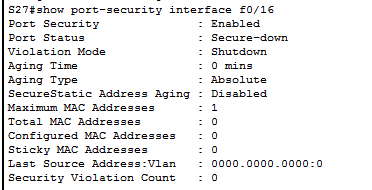


1. NTP

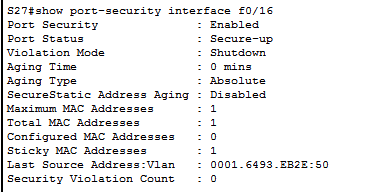


Paso 12 -LAN

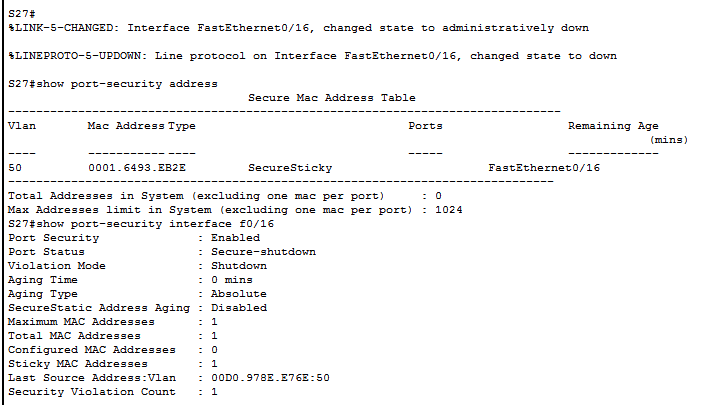
1. Seguridad de puertos de un switch



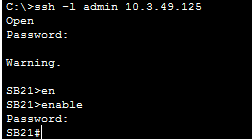
En esta primera imagen se ingresa a la interfaz con el proposito de ver el estado actual



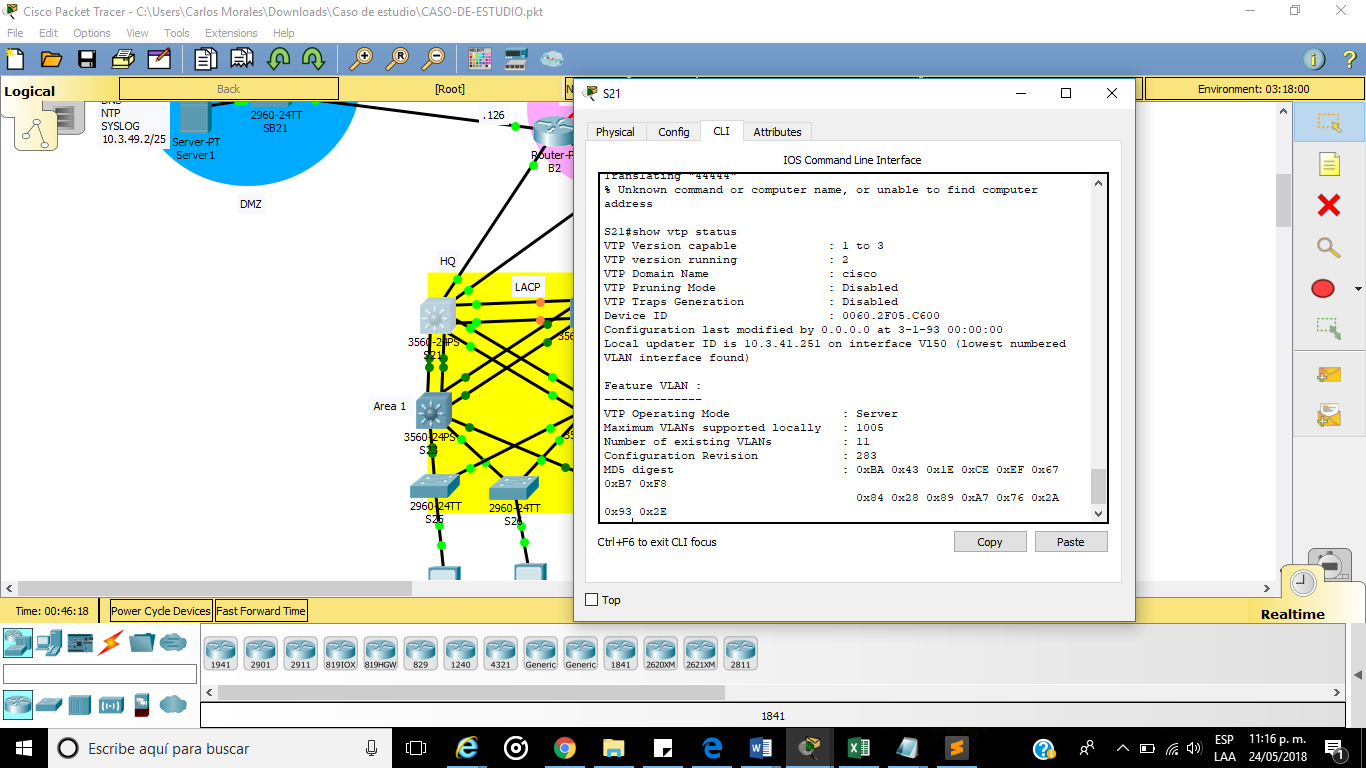
Le conectamos una pc para que detecte su MAC.

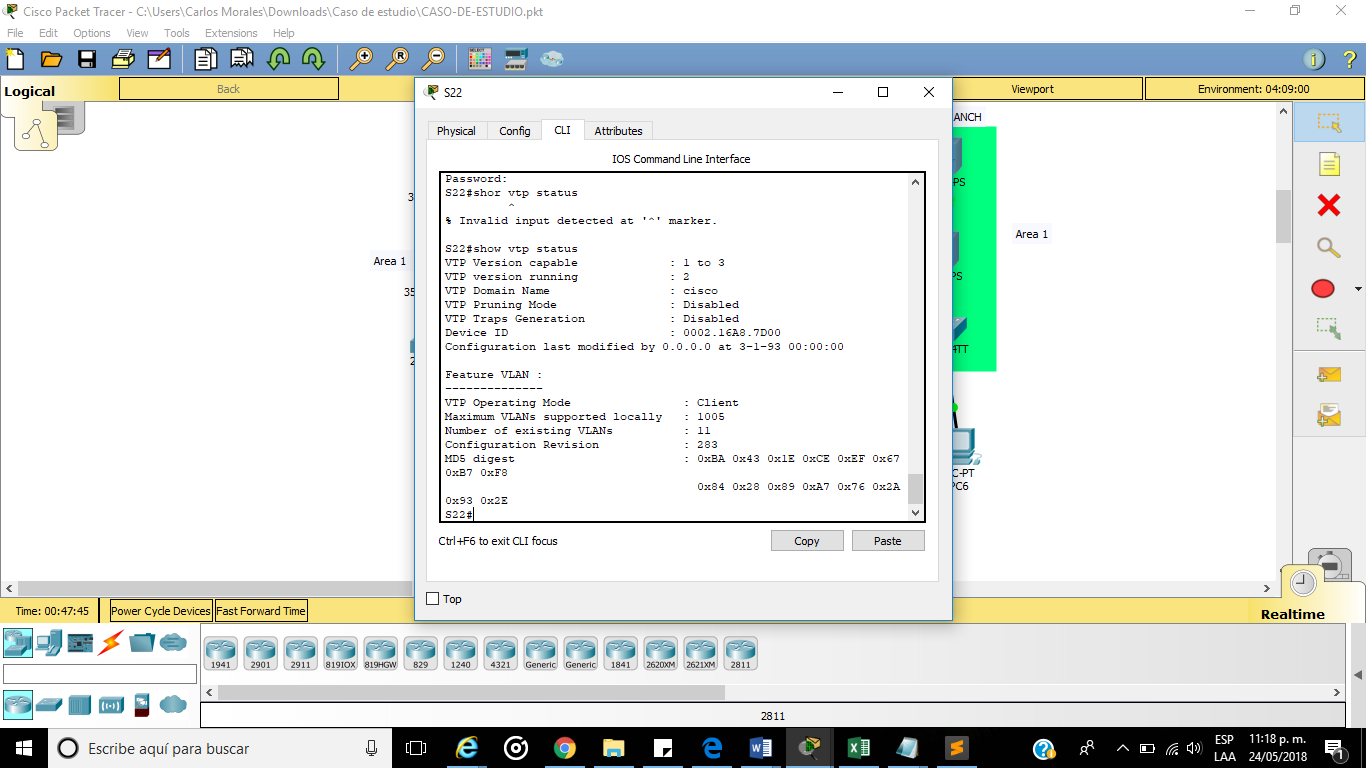
 Desconectamos la pc mencionada y conectamos otra y vemos que la interfaz de apaga de forma automatica y ademas aumenta el contador de violacion de seguridad.

1. Acceso Remoto

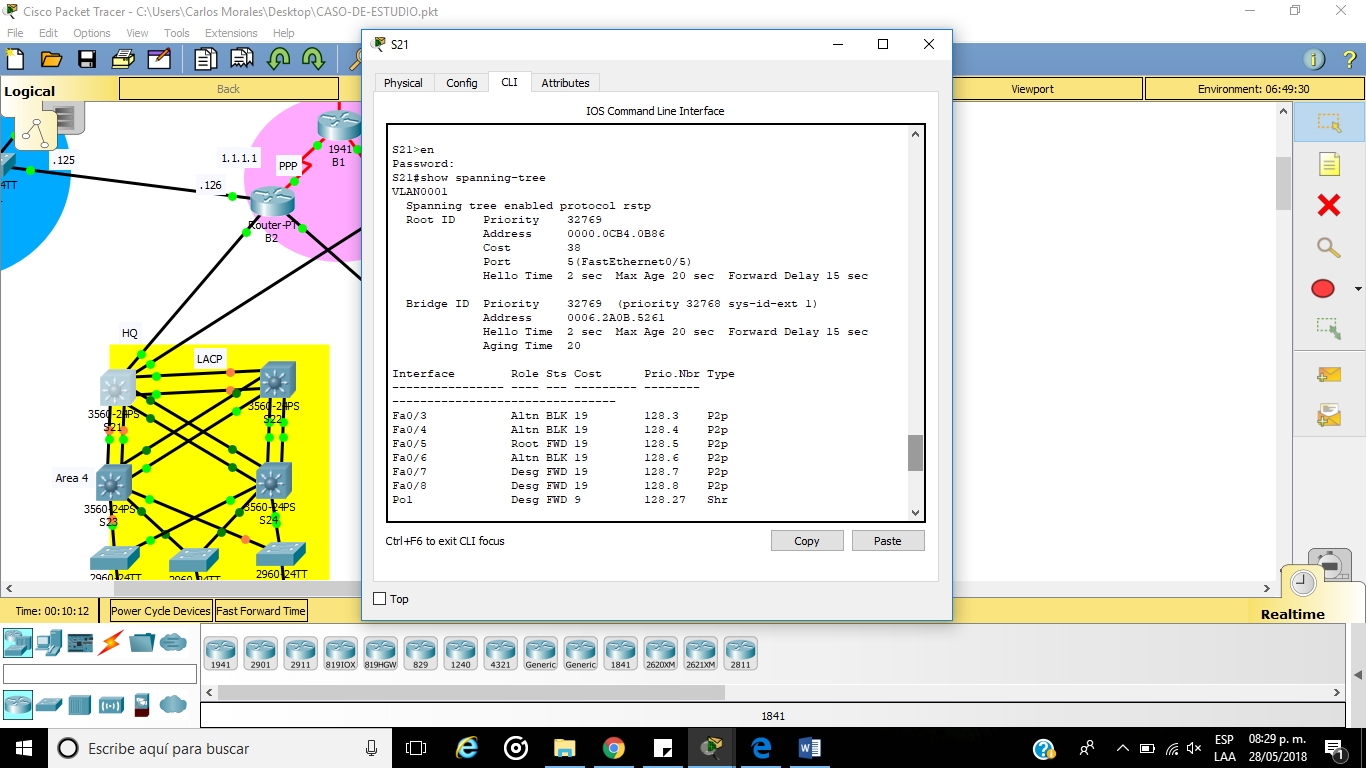


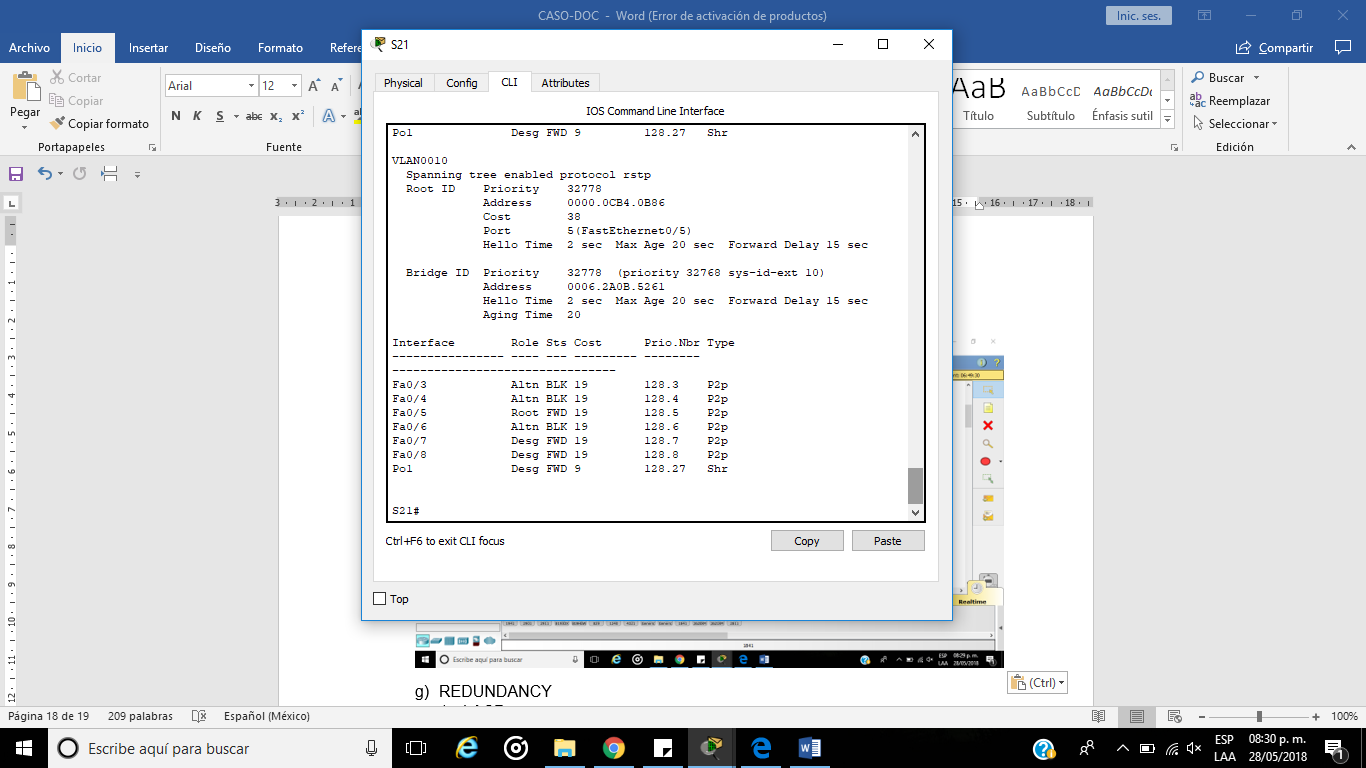
1. VTP



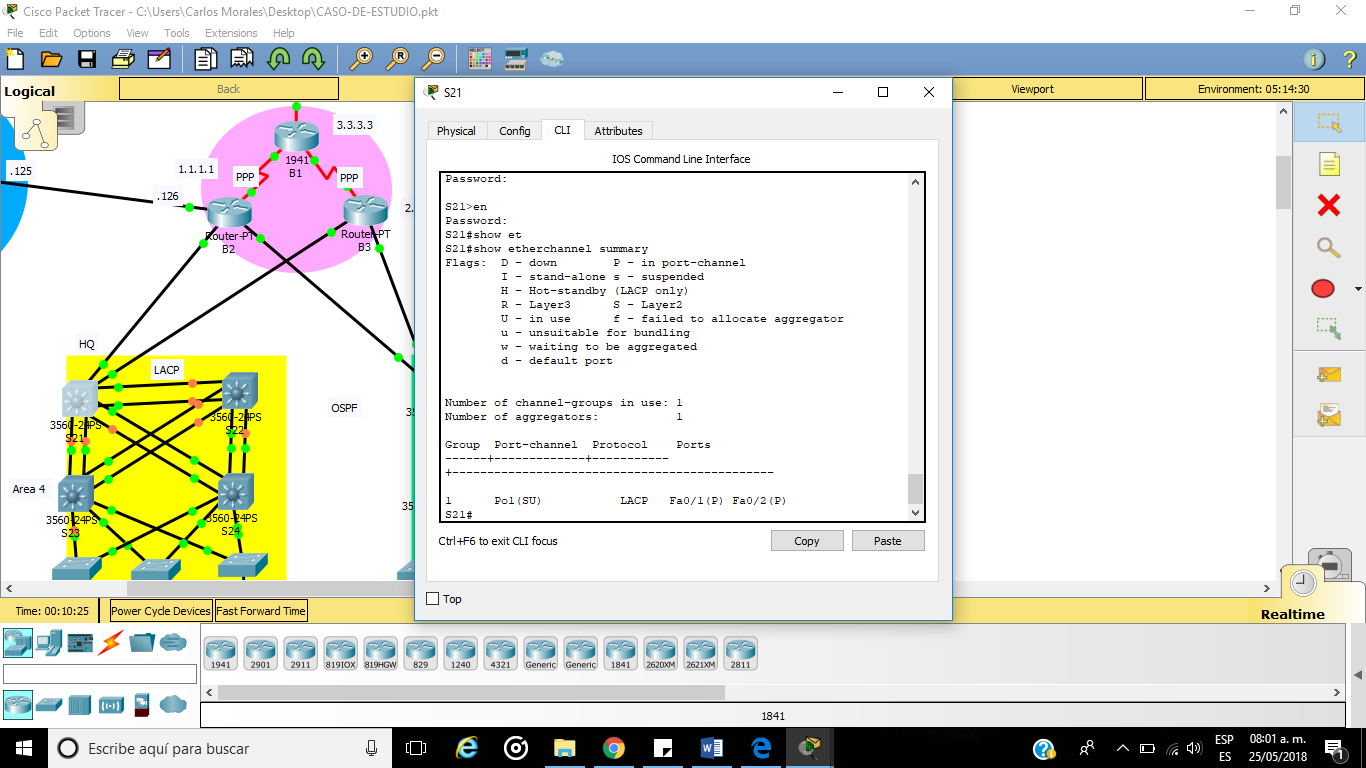


1. DTP
2. STP

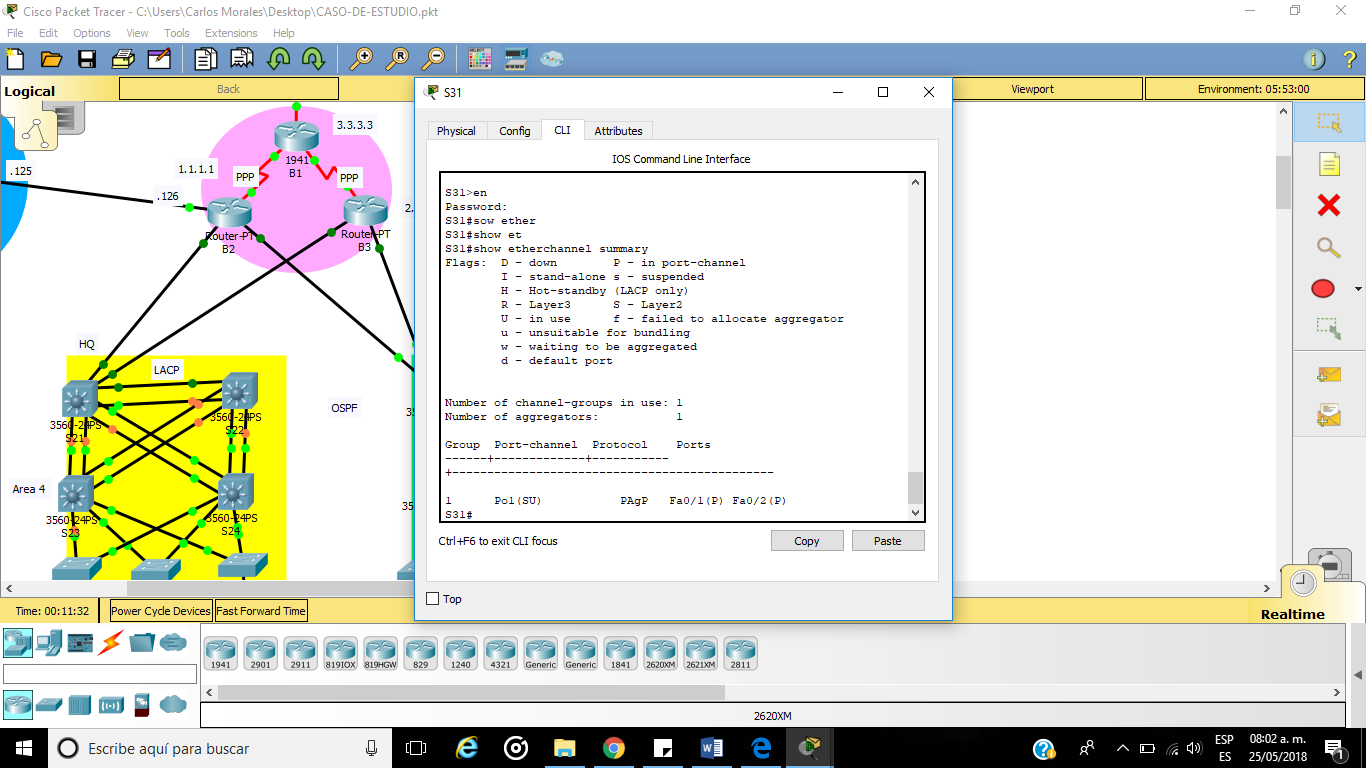




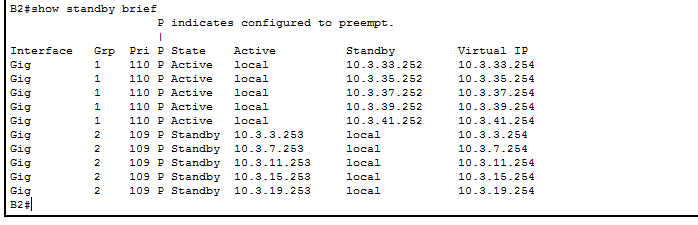
1. REDUNDANCY
2. LACP



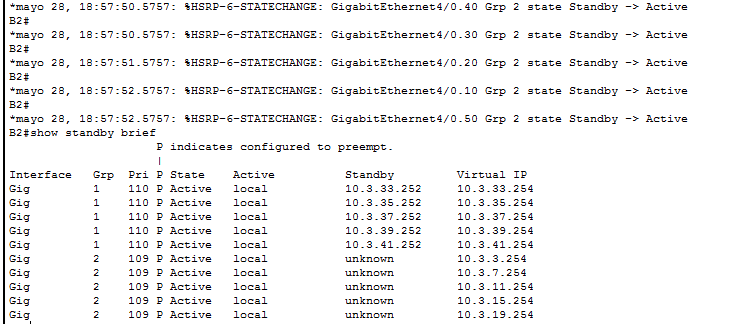
1. PAgP



1. HSRP

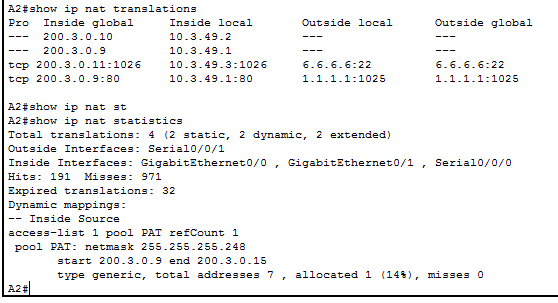


En esta imagen vemos las interfaces que pertenecen al grupo 2 estan en modo standy.



Pero una vez que se desconecta el cable donde estan las subinterfaces 10.3.3.253, 10.3.7.253, 10.3.11.253, 10.3.15.253 y 10.3.19.253 vemos que las interfaces del router en el que estamos pasan a modo activo.

Nat



Una de las pruebas que se hizo para el nat fue a travez de los comandos:

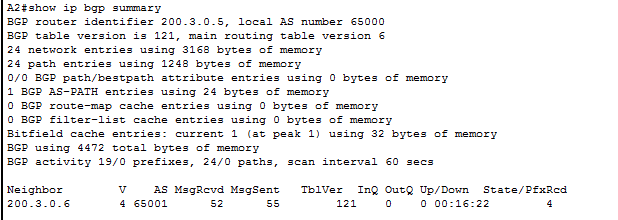
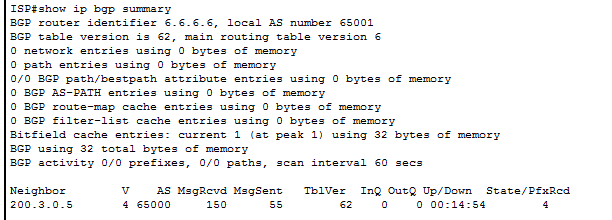
Show ip nat translations:

Muestra las truducciones que ha hecho el nat. Este comando lo usamos junto con un ping para probar que se hicieran bien las traducciones y efectivamente funciono.

Show ip nat statistics

Muestra informacion relevante del nat.

BGP



Como podemos ver se uso el comando show ip bgp summary para ver mas que nada los vecinos del bpg ya que en esta parte se nos muestra tambien el sistema autonomo de cada uno de los router donde se configuro bgp que fueron en los routers ISP y A2.