

TECNOLOGIAS DE REDES WAN
Segunda Evaluación

Nombre: _____
Paralelo: _____

Calificación:

--

1. Defina brevemente los siguientes términos (30 puntos)

- a) EUI-64

- b) NAT estático

- c) BOOTP

- d) Método “Sistemático”

- e) ACL Nombrada Extendida

- f) VPN “Sitio a Sitio”

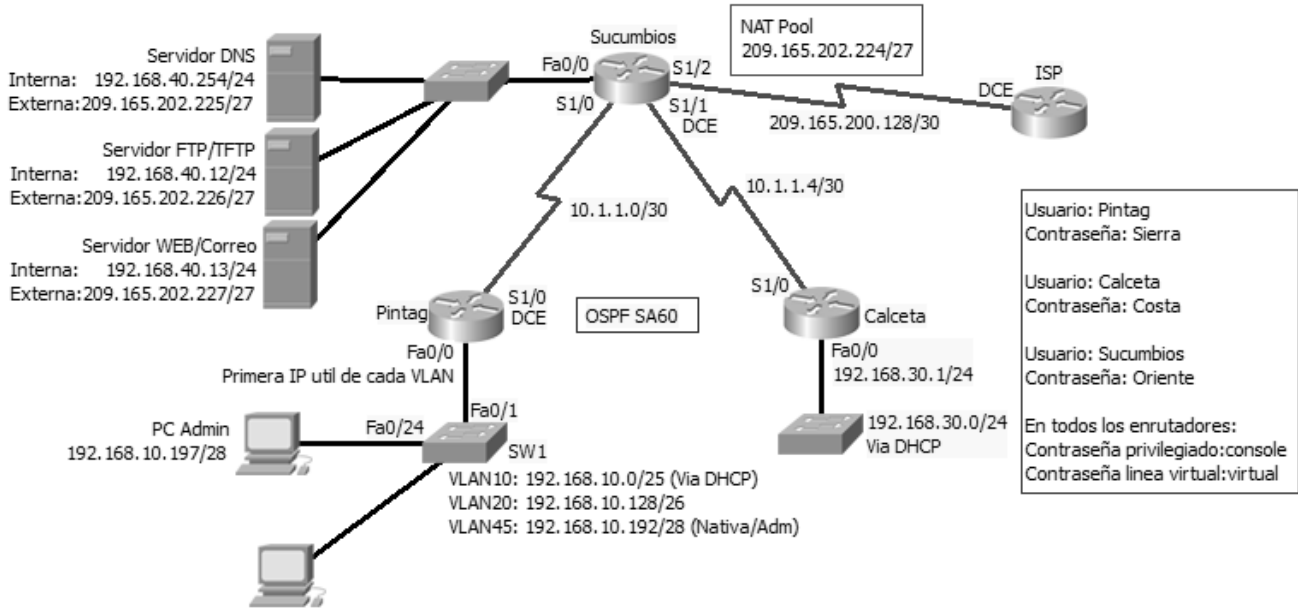
- g) Teletrabajador

- h) Puerta de Enlace

- i) Servidor DNS

- j) ICMP

2. Basándose en la topología mostrada en la figura, identificar y describir los errores en la configuración de los enrutadores y describir al menos una posible solución para cada uno de ellos (20 puntos)



```
Sucumbios#show running-config
hostname Sucumbios
!
username Sucumbios password 0 Oriente
!
interface FastEthernet0/0
 ip address 192.168.40.1 255.255.255.0
 ip nat inside
!
interface Serial1/0
 ip address 10.1.1.2 255.255.255.252
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username Sucumbios password 0 Oriente
 ip nat inside
!
interface Serial1/1
 ip address 10.1.1.5 255.255.255.252
 encapsulation ppp
 ip nat inside
!
interface Serial1/2
 ip address 209.165.200.130 255.255.255.252
 ip nat outside
!
router ospf 60
 redistribute static
 passive-interface default
 no passive-interface Serial1/0
 no passive-interface Serial1/1
 network 192.168.40.0 0.0.0.255 area 0
 network 10.1.1.0 0.0.0.3 area 0
 network 10.1.1.4 0.0.0.3 area 0
!
ip nat pool NAT 209.165.202.228 209.165.202.254 netmask 255.255.255.224
ip nat inside source list ACCESO pool NAT
ip nat inside source static 192.168.40.254 209.165.202.225
ip nat inside source static 192.168.40.13 209.165.202.226
ip nat inside source static 192.168.40.12 209.165.202.227
ip route 0.0.0.0 0.0.0.0 Serial1/2
!
ip access-list standard ACCESO
 permit 192.168.10.0 0.0.0.255
 permit 192.168.30.0 0.0.0.255
!
line con 0
 login local
line vty 0 4
 password virtual
 login
!
end
```

<pre>Pintag#show running-config hostname Pintag ! ip dhcp excluded-address 192.168.10.1 192.168.10.5 ! ip dhcp pool VLAN10 network 192.168.10.0 255.255.255.128 default-router 192.168.10.1 dns-server 192.168.40.254 ! username Pintag password 0 Sierra username Sucumbios password 0 Oriente ! interface FastEthernet0/0 no ip address ! interface FastEthernet0/0.10 encapsulation dot1Q 10 ip address 192.168.10.1 255.255.255.128 ! interface FastEthernet0/0.20 encapsulation dot1Q 20 ip address 192.168.10.129 255.255.255.192 ! interface FastEthernet0/0.45 encapsulation dot1Q 45 native ip address 192.168.10.193 255.255.255.240 ! interface Serial1/0 ip address 10.1.1.1 255.255.255.252 encapsulation ppp ppp authentication pap ppp pap sent-username Pintag password 0 Sierra clock rate 125000 ! router ospf 60 passive-interface default no passive-interface Serial1/0 network 192.168.10.0 0.0.0.255 area 0 network 10.1.1.0 0.0.0.3 area 0 ! line con 0 login local line vty 0 4 password virtual login ! end</pre>	<pre>Calceta#show running-config hostname Calceta ! ip dhcp pool LAN30 network 192.168.30.0 255.255.255.0 default-router 192.168.30.1 dns-server 192.168.40.254 ! username Calceta password 0 Costa ! interface FastEthernet0/0 ip address 192.168.30.1 255.255.255.0 ! interface Serial1/0 ip address 10.1.1.6 255.255.255.252 encapsulation ppp ! router ospf 60 log-adjacency-changes passive-interface default no passive-interface Serial1/0 network 10.1.1.4 0.0.0.3 area 0 network 192.168.30.0 0.0.0.255 area 0 ! line con 0 login local line vty 0 4 password virtual login ! end ISP#show running-config ! hostname ISP ! interface Serial1/0 ip address 209.165.200.129 255.255.255.252 clock rate 125000 ! ip route 209.165.202.224 255.255.255.224 Serial1/0 ! end</pre>
<p>A)</p>	
<p>B)</p>	
<p>C)</p>	
<p>D)</p>	

3. Basándose en la topología mostrada en el tema anterior, escribir los comandos para configurar y aplicar las ACLs requeridas para cumplir con los siguientes requerimientos. Se deberá especificar en que dispositivo se esta trabajando. (30 puntos)

Requerimientos:

- Todos los enrutadores permiten acceso remoto únicamente a la PC Admin.
- Se debe impedir la suplantación de identidad de dirección IP origen en todos los enlaces LAN.
- Únicamente las redes VLAN45 y VLAN 20 de Pintag pueden acceder al servicio FTP
- Todas las redes excepto VLAN10 de Pintag pueden tener servicio TFTP, y DNS
- Todas las redes excepto la LAN de Calceta pueden acceder al Correo Electrónico.
- La red VLAN20 de Pintag es la única con acceso restringido al servicio WEB.
- La red VLAN10 de Pintag tiene prohibido contactar a las redes VLAN20 de Pintag y LAN de Calceta
- VLAN45 puede ingresar a cualquier red por cualquier medio.
- Los servidores únicamente pueden dar el servicio para el cual han sido programados.
- El Servicio FTP es exclusivo para la red interna de la compañía.
- Por favor recordar que algunos segmentos de red reciben dirección IP de forma automática

4. Describa detalladamente el proceso de obtención de direcciones de red usando un Servidor DHCP que no se encuentra en el mismo segmento de red. Por favor incluir un gráfico y un ejemplo. (20 puntos)