

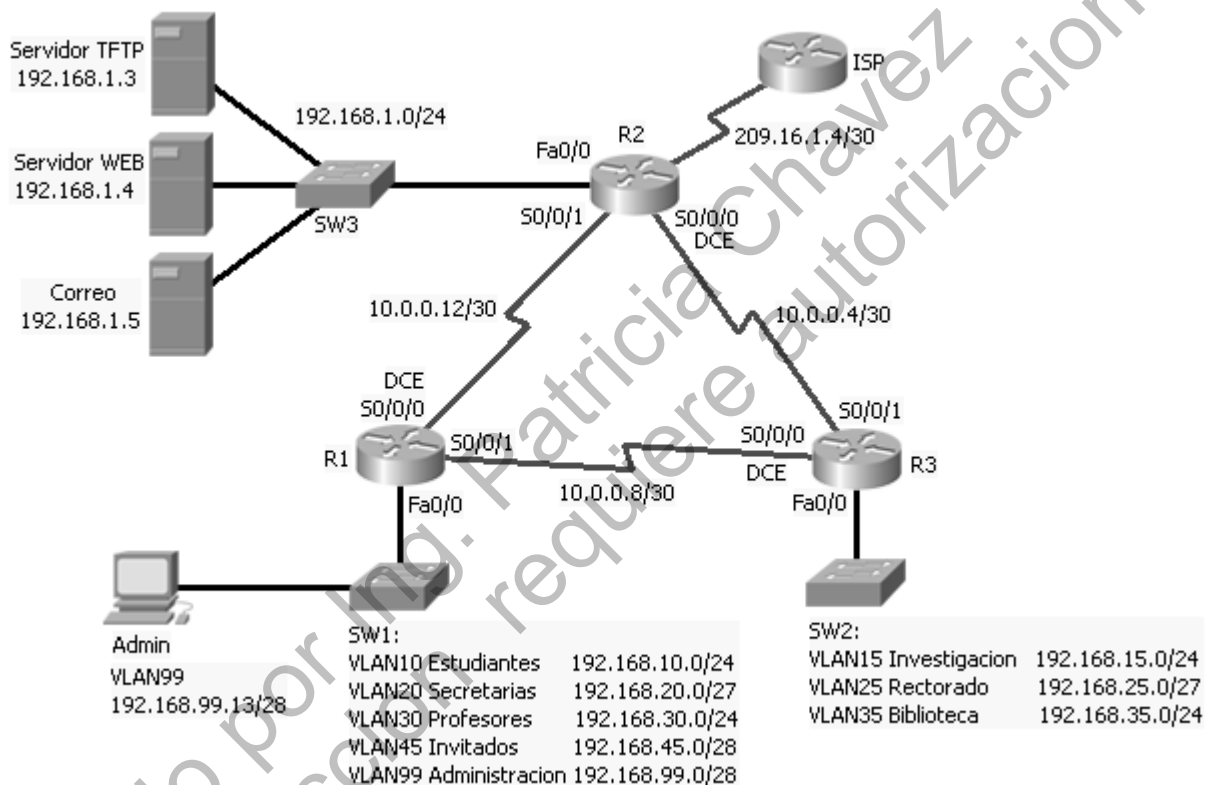
**TECNOLOGIAS DE REDES WAN
EXAMEN FINAL**

Nombre: _____

Laboratorios:	
Practico:	
Examen:	
Nota Final:	

TEMA 1 (40 puntos)

Basándose en la Topología mostrada, escribir los comandos para configurar y aplicar las ACLs necesarias para cumplir con los requerimientos dados. Se deberá especificar en que dispositivo se esta trabajando.

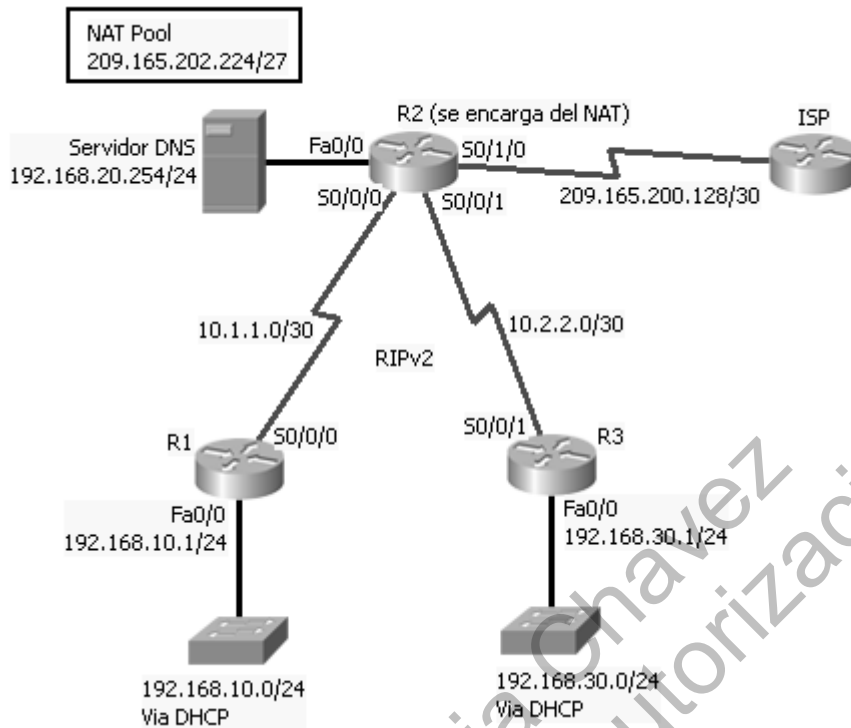


Requerimientos:

- Todos los enrutadores permiten acceso remoto únicamente a la PC Admin.
- Se debe impedir la suplantación de identidad de la dirección IP origen en todos los enlaces que no se conecten a los otros enrutadores
- Únicamente los computadores correspondientes a las redes “Secretarias”, “Profesores”, “Investigación”, “Rectorado” y “Administración” pueden tener servicio TFTP.
- Todos los computadores tienen acceso al servicio WEB y de Correo Electrónico.
- Los computadores de las redes “Biblioteca”, “Estudiantes” e “Invitados” tienen prohibido contactar a las redes “Secretarias”, “Profesores”, “Investigación”, “Rectorado” y “Administración”
- La red de Administración puede ingresar a cualquier red.
- Excepto por la red “Administración”, ninguna red le puede hacer ping o telnet a los servidores.
- Excepto por la red “Administración”, ninguna red le puede hacer ping o telnet a los dispositivos de la red “Investigación”.

TEMA 2 (15 puntos)

En base al Diagrama de la Red, encontrar los errores en la siguiente configuración.



```
R1#show running-config
hostname R1
!
interface FastEthernet0/0
ip address 192.168.10.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
ip address 10.1.1.1 255.255.255.252
clock rate 64000
!
interface Serial0/0/1
no ip address
shutdown
!
router rip
version 2
passive-interface FastEthernet0/0
network 10.0.0.0
network 192.168.20.0
no auto-summary
!
ip classless
!
ip dhcp excluded-address 192.168.10.2 192.168.10.9
!
ip dhcp pool R1LAN
network 192.168.10.0 255.255.255.0
default-router 192.168.30.1
dns-server 192.168.20.254
!
banner motd ^AUTHORIZED ACCESS ONLY!^C
!
line con 0
password cisco
login
line vty 0 4
password cisco
login
end
```

```
R3#show running-config
hostname R3
!
interface FastEthernet0/0
ip address 192.168.30.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
!
interface Serial0/0/1
ip address 10.2.2.2 255.255.255.0
!
router rip
version 2
passive-interface FastEthernet0/0
network 10.0.0.0
network 192.168.30.0
no auto-summary
!
ip classless
!
ip dhcp excluded-address 192.168.30.1 192.168.30.9
!
ip dhcp pool R3LAN
network 192.168.30.0 255.255.255.0
default-router 192.168.30.1
dns-server 172.168.20.254
!
banner motd ^AUTHORIZED ACCESS ONLY!^C
!
line con 0
password cisco
login
line vty 0 4
password cisco
login
!
end
```

```

R2#show running
hostname R2
!
interface FastEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.224
 ip nat inside
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 ip nat inside
 clock rate 64000
!
interface Serial0/1/0
 ip address 209.165.200.129 255.255.255.252
 ip nat outside
!
interface Serial0/1/1
 no ip address
 shutdown
!
router rip
 version 2
 passive-interface Serial0/0/0
 passive-interface Serial0/1/0
 network 10.0.0.0
 default-information originate
 no auto-summary
!
ip nat pool R2POOL 209.165.202.224 209.165.202.253
 netmask 255.255.255.0
 ip nat inside source list R2NAT pool R2POOL
 ip nat inside source static 192.168.30.254
 209.165.202.254
 ip classless
 ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ip access-list standard R2NAT
 permit 192.168.10.0 0.0.0.255
 permit 192.168.20.0 0.0.0.255
 permit 192.168.30.0 0.0.0.127
!
banner motd ^AUTHORIZED ACCESS ONLY!^C
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
    
```

TEMA 3 (10 puntos)

Enlace los comandos con las definiciones adecuadas.

A	no access-list 10
B	ip helper-address 192.168.1.13
C	access-class 21 in
D	ip nat inside
E	ip access-list extended AMIGOS
F	access-list 1 permit any
G	ip nat inside source static A B
H	debug ip nat
I	ip access-group 1 in
J	ip nat inside source list 1 pool AB
K	ip dhcp pool LAN1
L	no access-list 101

ACL que permitir el acceso de cualquier paquete	
Elimina una lista de acceso IP extendida	
Ubica una ACL estándar a la entrada de la interfaz	
Establece el banco de direcciones para DHCP	
Traduce la dirección A en dirección B	
Indica que por esa interfaz entran las direcciones privadas	
Permite visualizar la traducción de direcciones IP	
Establece la dirección para reenviar las peticiones DHCP	
Ubica una ACL estándar para controlar el acceso virtual	
Crea una ACL nombrada	

TEMA 4 (10 puntos)

Defina los siguientes términos:

1. ACL

2. DSL

3. VPN

4. DHCP

5. NAT

TEMA 5 (10 puntos)

Indique el rango de frecuencia, alcance y velocidad de los estándares inalámbricos IEEE802.11a, IEEE802.11b, IEEE802.11g y IEEE802.11n.

TEMA 6 (15 puntos)

Describa detalladamente la importancia de establecer una “Linea Base de la Red”. De ejemplo de posibles usos

Elaborado por Ing. Patricia Chavez
La reproduccion requiere autorizacion previa