ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN

TECNOLOGÍAS DE REDES WAN
SEGUNDA EVALUACIÓN - PRIMER TÉRMINO 2016

Nombre: _____ **Calificación:**

Paralelo: _____

- **Lea detenidamente las preguntas y conteste de acuerdo a los conocimientos adquiridos. El examen será calificado sobre 100 puntos, cada pregunta será ponderada en 5 puntos.**

1) ¿Qué es una política de seguridad a nivel empresarial?

2) De acuerdo a las definiciones mostradas en la tabla, indicar el Término correcto.

Definición	Término
Persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.	
Persona que manipula la red telefónica para que realice una función que no está permitida.	
Persona que envía grandes cantidades de mensajes de correo electrónico no solicitado.	
Se usan en lugares donde no está disponible el acceso a Internet terrestre o en instalaciones temporarias que están en continuo movimiento.	
Persona que busca vulnerabilidades en los sistemas o en las redes y, a continuación, informa estas vulnerabilidades a los propietarios del sistema para que las arreglen.	

3) El administrador del enrutador R1, ha denotado que el usuario "admin" muestra la contraseña en texto sin cifrar, ¿Qué comando propone para mejorar la seguridad a nivel global para todas las contraseñas del enrutador?

```
R1(config)#username admin password cisco123
```

4) En base a la parámetro mostrado, explique su función.

```
R1#copy startup-config tftp
```

5) Explique dónde se deben aplicar las ACL estándar y extendida, para un filtrado de paquetes eficiente.

6) Especifique las partes que componen una dirección IP versión 6.

Docente FIEC Msig. Adriana Collaguazo Jaramillo

7) Se ha presenta un error en la definición de la lista de control de acceso BLOQUEO_APLICACION del enrutador "NET", siendo necesario agregar una nueva sentencia para denegar el tráfico SMTP desde cualquier red hacia la dirección de host 172.16.0.10. Indique el comando apropiado para agregar la nueva con el orden secuencial utilizado, en base a la configuración mostrada.

```
NET#show access-lists
Extended IP access list BLOQUEO_APLICACION
    10 deny tcp any host 172.16.0.10 eq ftp
    20 deny tcp any host 172.16.0.10 eq telnet
    30 deny tcp any host 172.16.0.10 eq www
    40 permit ip any any
```

8) En el enrutador R1 se solicita que defina y aplique una lista de control de acceso para permitir el tráfico telnet sólo desde las subredes 192.168.1.0/24, 192.168.2.0/24.

9) Indique el tipo de VPN que se debe utilizar para que el personal de Ingenieros de campo que se desplazan continuamente con sus laptop y herramientas entre las diferentes oficinas de la empresa puedan acceder a los recursos de la intranet de la Empresa. Argumente su respuesta:

10) Indique el tipo de tecnología de acceso a Internet que contrataría para una oficina ubicada en Galápagos Isla San Cristóbal, con un ancho de banda de 1 Mbps.

11) Explique brevemente el funcionamiento del protocolo DHCP, especificando los mensajes que se intercambian entre el cliente y servidor.

12) Indique el tipo de NAT que utilizaría, si diez PCs de una red LAN necesitan navegar con la única dirección IP pública de la interfaz WAN del enrutador.

13) Resuma la dirección IPv6 2001:0000:0000:0000:ABCD:0000:0000:1223, de acuerdo a las reglas establecidas.

14) Indique la longitud del prefijo más utilizado en direccionamiento IPv6.

15) ¿Cuántos bits contienen una dirección IPv6?

---

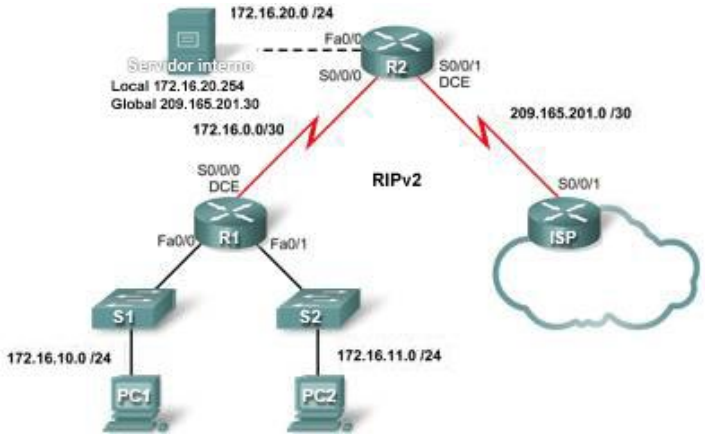
16) Indique el nombre del tipo de diagrama de topología, donde se encuentran detallan los modelos de los enrutadores, conmutadores, cableado, interfaces físicas con sus respectivas conexiones.

---

17) ¿Qué método de resolución de problemas, debo utilizar cuando recibo un reporte de un cliente que indica que no tiene ningún servicio en la red?

En base a las configuraciones mostradas, siendo el enrutador R2 el servidor DHCP. Responda a las siguientes preguntas:

18) Identifique los errores por los cuales la red no funciona, y proponga una solución con los comandos apropiados incluyendo el modo de configuración.



R1#show running-config hostname R1 interface FastEthernet0/0 ip address 172.16.10.1 255.255.255.0 ip helper-address 172.16.0.2 no shutdown interface FastEthernet0/1 ip address 172.16.11.1 255.255.255.0 ip helper-address 172.16.0.77 no shutdown interface Serial0/0/0 ip address 172.16.0.1 255.255.255.252 clock rate 125000 no shutdown router rip version 2 passive-interface default network 172.16.0.0 no auto-summary banner motd $ ********** !!!AUTHORIZED ACCESS ONLY!!! **********! line con 0 password cisco logging synchronous login	R2#show running-config hostname R2 enable secret class ip dhcp excluded-address 172.16.10.1 172.16.10.3 ip dhcp excluded-address 172.16.11.1 172.16.11.3 ip dhcp pool R1_LAN10 network 172.16.10.0 255.255.255.0 default-router 172.16.50.1 dns-server 172.16.20.254 ip dhcp pool R1_LAN11 network 172.16.11.0 255.255.255.0 default-router 172.16.11.1 dns-server 172.16.20.254 no ip domain lookup int fa0/0 ip address 172.16.20.1 255.255.255.0 ip nat inside no shutdown interface Serial0/0/0 ip address 172.16.0.2 255.255.255.252 ip nat inside no shutdown interface Serial0/0/1 ip address 209.165.201.1	ISP#show running-config hostname ISP enable secret class interface Serial0/0/1 ip address 209.165.201.2 255.255.255.252 no shutdown ip route 209.165.201.0 255.255.255.224 Serial0/0/1 banner motd $ ********** ******* !!!AUTHORIZED ACCESS ONLY!!! ********** ******* $ line con 0 password cisco logging synchronous login line vty 0 4 password cisco logging synchronous login end

line vty 0 4 password cisco logging synchronous login end	255.255.255.252 ip nat outside clock rate 125000 no shutdown router rip version 2 network 172.16.0.0 default-information originate no auto-summary ip route 0.0.0.0 0.0.0.0 209.165.201.2 ip nat pool NAT_POOL 209.165.201.9 209.165.201.14 netmask 255.255.255.248 ip nat inside source list NAT_ACL pool NAT_POOL overload ip nat inside source static 172.16.20.254 209.165.201.30 ip access-list standard NAT_ACL permit 172.16.10.0 0.0.0.255 permit 172.16.11.0 0.0.0.255 banner motd $ ********** **** !!!AUTHORIZED ACCESS ONLY!!! ********** **** $ line con 0 password cisco logging synchronous login line vty 0 4 password cisco logging synchronous login end	

Error 1:	Solución 1:
Error 2:	Solución 2:
Error 3:	Solución 3:

19) Indique qué tipo de NAT utiliza el enrutador R2. _____

20) Indique que función realiza el comando passive-interface default aplicado en el enrutador R1.

_____

_____

_____