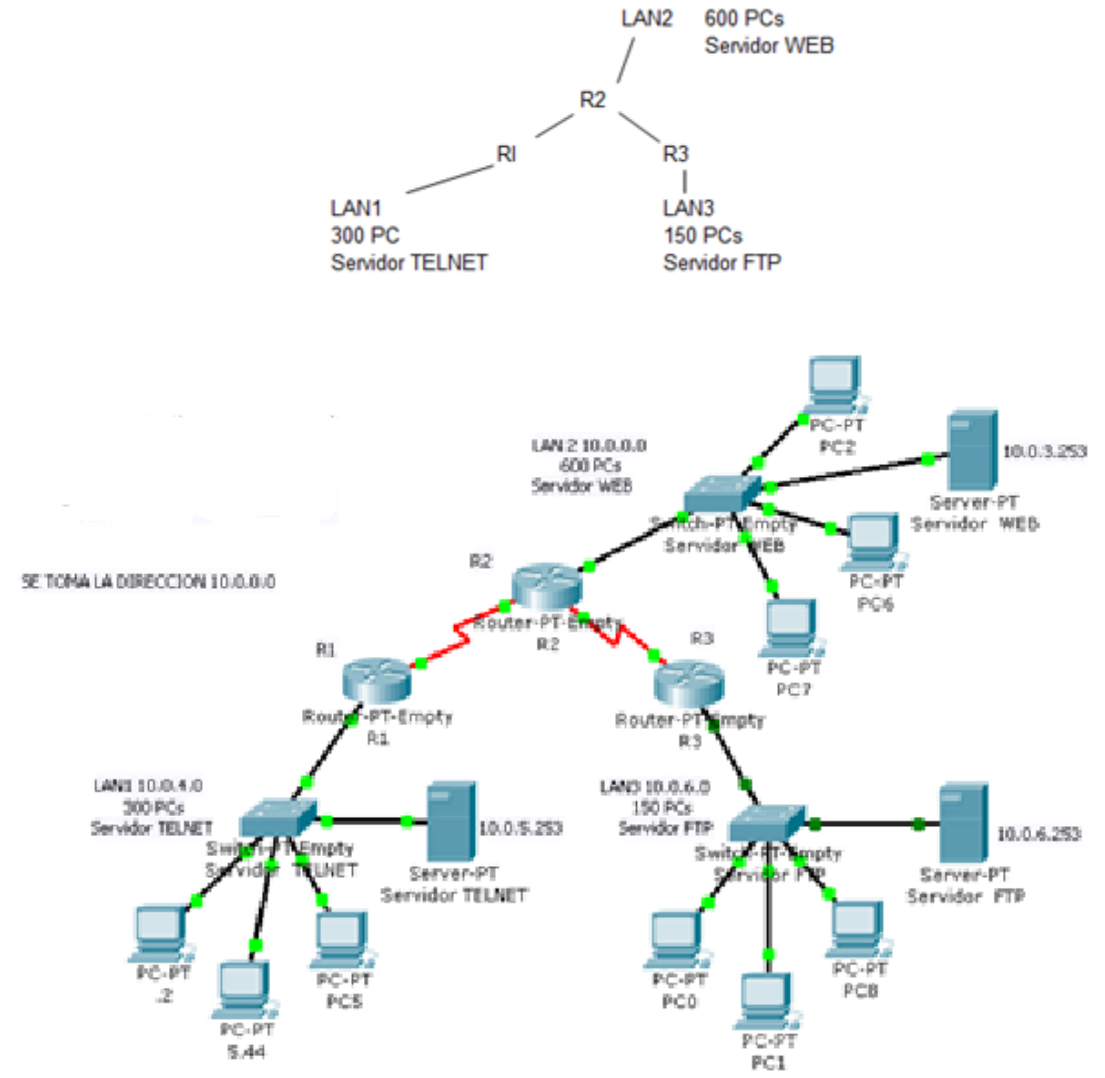
EJERCICIO LISTAS DE CONTROL DE ACCESO

Condiciones:

- Últimos 100 PCs de LAN 1 tienen acceso a servidor WEB
- Primeros 100 PCs de LAN 2 se comunican con LAN 3. Los otros no.
- No se permite acceso por TELNET a ningún router.
- No se permite PING al servidor WEB.



Solución:

SUBNETEO DE LA RED

Se toma la dirección Ip 10.0.0.0/8 para realizar el subneteo. En total son 5 subredes en la configuración que se muestra en el segundo gráfico, tomando las 3 LAN y los 2 enlaces sériele entre los routers.

La LAN 1 necesita 300 PCs, la LAN 2 600 PCS, LAN 3 150 PCs, cada enlace 2+2 Ip contando las subredes y la broadcast.

Se usó VLSM para el subneteo:

Tomamos la LAN 2 que es la de mayor número de PCs (600 host). Para ese número de host necesitamos 10 bits con no alcanza.

Luego tenemos: IP 10.0.0.0 macara 255.0.0.0

10 bit para host y la nueva mascara es:

255.255.252.0 11111111.11111111.11111100.00000000

Obtenemos la siguiente tabla:

	Rango				
IP de subred	**Primer host**	**Ultimo host**	**Broadcast**	**Mascara**	
10.0.0.0	10.0.0.1	10.0.3.254	10.0.5.255	255.255.252.0	LAN 2
10.0.4.0	10.0.4.1	10.0.7.254	10.0.7.255	255.255.252.0	
10.0.8.0	10.0.8.1	10.0.11.254	10.0.11.255	255.255.252.0	
10.0.12.0	10.0.12.1	10.0.15.254	10.0.15.255	255.255.252.0	
…	…	…	…	…	

Tomamos la primera subred para la LAN 2. Ahora se toma la siguiente subred para los 300 host de la LAN 1.

Para 300 host necesitamos 9 bits con no alcanza.

Luego tenemos: IP 10.0.4.0 macara 255.255.252.0

9 bit para host y la nueva mascara es:

255.255.254.0 11111111.11111111.11111110.00000000

Obtenemos la siguiente tabla: solo tenemos dos subredes

	Rango				
IP de subred	**Primer host**	**Ultimo host**	**Broadcast**	**Mascara**	
10.0.4.0	10.0.4.1	10.0.5.254	10.0.5.255	255.255.254.0	LAN 1
10.0.6.0	10.0.6.1	10.0.7.254	10.0.7.255	255.255.254.0	

Tomamos la primera subred para la LAN 1. Ahora se toma la siguiente subred para los 150 host de la LAN 3.

Para 150 host necesitamos 9 bits con no alcanza.

Luego tenemos: IP 10.0.6.0 macara 255.255.254.0

9 bit para host y la nueva mascara es:

255.255.255.0 11111111.11111111.11111111.00000000

Obtenemos la siguiente tabla: solo tenemos dos subredes

	Rango				
IP de subred	**Primer host**	**Ultimo host**	**Broadcast**	**Mascara**	
10.0.6.0	10.0.6.1	10.0.6.254	10.0.5.255	255.255.255.0	LAN 3
10.0.7.0	10.0.7.1	10.0.7.254	10.0.7.255	255.255.255.0	

Tomamos la primera subred para la LAN 3. Ahora se toma la siguiente subred para los enlaces de los routers.

Para los enlaces (dos) necesitamos 2 bits las dos asignables para cada router + la subred y la broadcast.

Luego tenemos: IP 10.0.7.0 macara 255.255.255.0

2 bit para host y la nueva mascara es:

255.255.255.252 11111111.11111111.11111111.11111100

Obtenemos la siguiente tabla: solo tenemos dos subredes

	Rango				
IP de subred	**Primer host**	**Ultimo host**	**Broadcast**	**Mascara**	
10.0.7.0	10.0.7.1	10.0.7.2	10.0.7.3	255.255.255.252	Enlace 1
10.0.7.4	10.0.7.5	10.0.7.5	10.0.7.7	255.255.255.252	Enlace 2
10.0.7.8	10.0.7.9	10.0.7.10	10.0.7.11	255.255.255.252	
…	…	..	…	…	

Tomamos las dos primeras subredes para los enlaces. A continuación, se observan los enlaces de los routers.

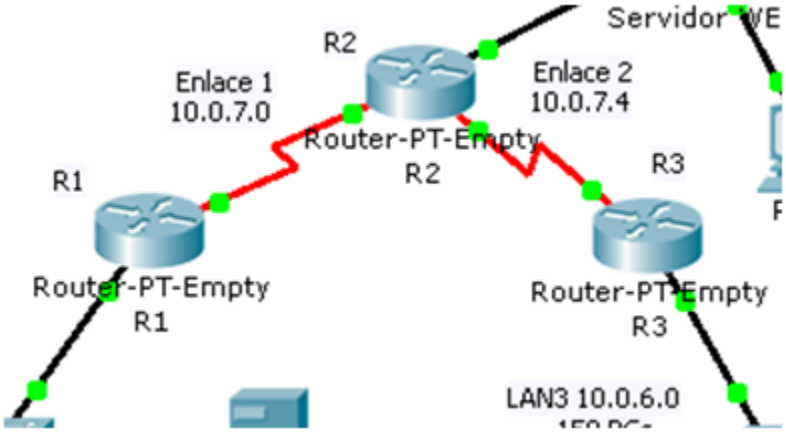


Tabla final de la RED

	Rango				
IP de subred	**Primer host**	**Ultimo host**	**Broadcast**	**Mascara**	
10.0.0.0	10.0.0.1	10.0.3.254	10.0.5.255	255.255.252.0	LAN 2
10.0.4.0	10.0.4.1	10.0.5.254	10.0.5.255	255.255.254.0	LAN 1
10.0.6.0	10.0.6.1	10.0.6.254	10.0.5.255	255.255.255.0	LAN 3
10.0.7.0	10.0.7.1	10.0.7.2	10.0.7.3	255.255.255.252	Enlace 1
10.0.7.4	10.0.7.5	10.0.7.5	10.0.7.7	255.255.255.252	Enlace 2

CONFIGURACIÓN DE LOS ROUTERS

Configuración Básica: Asignamos nombre de router, interfaces seriales etc.

Router R2:

Router#conf t

Router (config)#hostname R2

R2(config)#int fa0/0

R2 (config-if)#ip address 10.0.3.254 255.255.252.0

R2 (config-if)#no shutdown

R2(config-if)#exit

R2(config)#int se1/0

R2(config-if)#ip address 10.0.7.1 255.255.255.252

R2(config-if)#clock rate 56000

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#int se2/0

R2(config-if)#ip address 10.0.7.5 255.255.255.252

R2(config-if)#clock rate 56000

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#ip route 10.0.4.0 255.255.254.0 se1/0

R2(config)#ip route 10.0.6.0 255.255.255.0 se2/0

R2(config)#exit

Router R1:

Router#conf t

Router (config)#hostname R1

R1(config)#int fa0/0

R1 (config-if)#ip address 10.0.5.254 255.255.254.0

R1 (config-if)#no shutdown

R1(config-if)#exit

R1(config)#int se1/0

R1(config-if)#ip address 10.0.7.2 255.255.255.252

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#ip route 10.0.0.0 255.255.252.0 se1/0

R1(config)#ip route 10.0.6.0 255.255.255.0 se1/0

R1(config)#exit

Router R3:

Router#conf t

Router (config)#hostname R3

R3(config)#int fa0/0

R3 (config-if)#ip address 10.0.6.254 255.255.255.0

R3 (config-if)#no shutdown

R3(config-if)#exit

R3(config)#int se2/0

R3(config-if)#ip address 10.0.7.6 255.255.255.252

R3(config-if)#no shutdown

R3(config-if)#exit

R3(config)#ip route 10.0.0.0 255.255.252.0 se2/0

R3(config)#ip route 10.0.4.0 255.255.254.0 se2/0

R3(config)#exit

Configuración de ACLs:
Asignamos las listas a cada router dependiendo de las condiciones establecidas por el tutor.

Condición 1: Últimos 100 PCs de LAN 1 tienen acceso a servidor WEB

Se aplica una lista de control de acceso extendida cerca del origen, en este caso R1 (router 1).

Recordemos la LAN 1:

	Rango				
IP de subred	**Primer host**	**Ultimo host**	**Broadcast**	**Mascara**	
10.0.4.0	10.0.4.1	10.0.5.254	10.0.5.255	255.255.254.0	LAN 1

En este caso se nos pide permitir el acceso a WEB a los últimos 100 host de los 300 pro en realidad tenemos 511 host disponibles, entonces si tomamos los primeros 300 de estos los últimos 100 serían del host 10.0.4.200 al 10.0.5.44.

Para lograr esto se hace uso de la máscara wildcard de la siguiente manera:

	256	128	64	32	16	8	4	2	1		Wildcard Máximo	Wildcard a Utilizar
IP(10.0.4.200)	0	1	1	0	0	1	0	0	0		0.0.0.7	0.0.0.7
IP(10.0.4.208)	0	1	1	0	1	0	0	0	0		0.0.0.15	0.0.0.15
IP(10.0.4.224)	0	1	1	1	0	0	0	0	0		0.0.0.31	0.0.0.31
IP(10.0.5.0)	1	0	0	0	0	0	0	0	0		0.0.0.255	0.0.0.31
IP(10.0.5.32)	1	0	0	1	0	0	0	0	0		0.0.0.31	0.0.0.7
IP(10.0.5.40)	1	0	0	1	0	1	0	0	0		0.0.0.7	0.0.0.3
IP(10.0.5.44)	1	0	0	1	0	1	1	0	0		0.0.0.3	0.0.0.0

PASO 1:

Transformar a binario la IP de inicio (en este caso la 200)

PASO 2:

Sumar todos los 0 que se ubiquen al final del binario y que estén de forma continua (en la primera línea son los últimos 3 dígitos, en la segunda línea los últimos 4 dígitos, en la cuarta línea los últimos 5 dígitos, etc, etc, etc).

Esta suma te dará como resultado la wildcard más grande que puedes utilizar. NADA más grande que eso, podrías utilizar una wildcard menor, pero jamás una mayor.

PASO 3:

Suma la IP + la wildcard (en el caso de la primera línea 200 + 7 = 207), esto dará como resultado hasta que IP avanzo la wildcard (en este caso la 207, por lo tanto, la próxima línea de la ACL comenzara en la IP 208).

PASO 4:

Vuelve al paso 1 y repite hasta llegar al final del rango solicitado

Ahora vamos a observar la línea correspondiente a la Ip 10.0.5.0. Esto porque la wildcard más grande que podemos utilizar es la 255, pero con esto quedamos sobre el rango solicitado. Entonces utilizaremos una wildcard más pequeña, pero que se nos acerque lo más posible a nuestro destino (en este caso 10.0.5.44) por lo tanto utilizaremos la 31. Finalmente quiero explicar la última línea la Ip 10.0.5.44. Aquí hemos utilizado la wildcard 0 también conocida como de host ya que esta simplemente abarca una ip (en este caso la 10.0.5.44, para ser más claros 10.0.5.44 + 0 = 10.0.5.44).

La lista de acceso queda:

R1(config)#access-list 113 permit tcp 10.0.4.200 0.0.0.7 host 10.0.3.253 eq 80

R1(config)#access-list 113 permit tcp 10.0.4.208 0.0.0.15 host 10.0.3.253 eq 80

R1(config)#access-list 113 permit tcp 10.0.4.224 0.0.0.31 host 10.0.3.253 eq 80

R1(config)#access-list 113 permit tcp 10.0.5.0 0.0.0.31 host 10.0.3.253 eq 80

R1(config)#access-list 113 permit tcp 10.0.5.32 0.0.0.7 host 10.0.3.253 eq 80

R1(config)#access-list 113 permit tcp 10.0.5.40 0.0.0.3 host 10.0.3.253 eq 80

R1(config)#access-list 113 permit tcp 10.0.5.44 0.0.0.0 host 10.0.3.253 eq 80

R1(config)#access-list 113 deny tcp any host 10.0.3.253 eq 80

R1(config)#int f0/0

R1(config-if)#ip access-group 113 in

R1(config-if)#exit

Condición 2: Primeros 100 PCs de LAN 2 se comunican con LAN 3. Los otros no.

En este caso utilizamos el procedimiento anterior ya que se piden los primeros 100 host de esta LAN. Se aplica en el R2 (router 2). Recordemos la LAN 2.

	Rango				
IP de subred	**Primer host**	**Ultimo host**	**Broadcast**	**Mascara**	
10.0.0.0	10.0.0.1	10.0.3.254	10.0.5.255	255.255.252.0	LAN 2

El rango de host es 10.0.0.1 al 10.0.0.100.

Se obtiene la tabla:

	128	64	32	16	8	4	2	1		Wildcard Máximo	Wildcard a Utilizar
IP(10.0.0.1)	0	0	0	0	0	0	0	1		0.0.0.0	0.0.0.0
IP(.2)	0	0	0	0	0	0	1	0		0.0.0.1	0.0.0.1
IP(.4)	0	0	0	0	0	1	0	0		0.0.0.3	0.0.0.3
IP(.8)	0	0	0	0	1	0	0	0		0.0.0.7	0.0.0.7
IP(.16)	0	0	0	1	0	0	0	0		0.0.0.15	0.0.0.15
IP(.32)	0	0	1	0	0	0	0	0		0.0.0.31	0.0.0.31

IP(.64)	0	1	0	0	0	0	0	0		0.0.0.63	0.0.0.31
IP(.96)	0	1	1	0	0	0	0	0		0.0.0.31	0.0.0.3
IP(.100)	0	1	1	0	0	1	0	0		0.0.0.3	0.0.0.0

La lista de acceso queda:

R2(config)#access-list 114 permit ip 10.0.0.1 0.0.0.0 10.0.6.0 0.0.0.255

R2(config)#access-list 114 permit ip 10.0.0.2 0.0.0.1 10.0.6.0 0.0.0.255

R2(config)#access-list 114 permit ip 10.0.0.4 0.0.0.3 10.0.6.0 0.0.0.255

R2(config)#access-list 114 permit ip 10.0.0.8 0.0.0.7 10.0.6.0 0.0.0.255

R2(config)#access-list 114 permit ip 10.0.0.16 0.0.0.15 10.0.6.0 0.0.0.255

R2(config)#access-list 114 permit ip 10.0.0.32 0.0.0.31 10.0.6.0 0.0.0.255

R2(config)#access-list 114 permit ip 10.0.0.64 0.0.0.31 10.0.6.0 0.0.0.255

R2(config)#access-list 114 permit ip 10.0.0.96 0.0.0.3 10.0.6.0 0.0.0.255

R2(config)#access-list 114 permit ip 10.0.0.100 0.0.0.0 10.0.6.0 0.0.0.255

R2(config)#int s2/0

R2(config-if)#ip access-group 114 out

Condición 3: No se permite acceso por TELNET a ningún router.

R1(config)#access-list 113 deny tcp any any eq 23

R1(config)#access-list 113 permit ip any any

R2(config)#access-list 115 deny tcp any any eq telnet

R2(config)#access-list 115 permit ip any any

R2(config)# interface FastEthernet0/0

R2(config-if)# ip access-group 115 in

R3(config)#access-list 116 deny tcp any any eq telnet

R3(config)#access-list 116 permit ip any any

R3(config)# interface FastEthernet0/0

R3(config-if)# ip access-group 116 in

Condición 4: No se permite PING al servidor WEB.

Para esta lista se configura en los routers R1 y R3 lo siguiente:

R1(config)#access-list 112 deny icmp any 10.0.3.253 0.0.0.0

R1(config)#access-list 112 permit icmp any any

R1(config)#access-list 112 permit ip any any

R1(config)#int s1/0

R1(config-if)#ip access-group 112 out

R1(config-if)#exit

R3(config)#access-list 112 deny icmp any 10.0.3.253 0.0.0.0

R3(config)#access-list 112 permit icmp any any

R3(config)#access-list 112 permit ip any any

R3(config)#int s2/0

R3(config-if)#ip access-group 112 out

R1(config-if)#exit

De esta forma todos los hosts no podrán hacer PING al servidor WEB.