Instituto Tecnoló



**“Examen subnetting”**

Recientemente la “Universidad de las Américas”, uno de los clientes más importantes, ha solicitado nuestros servicios para diseñar un esquema de direccionamiento con máscaras de longitud variable que cumpla con los requerimientos de su red. La dirección de red asignada es: **175.40.192.0 / 18** (dirección / máscara). **(48 puntos)**

La topología de la “Universidad de las Américas” y sus necesidades de conectividad están representadas en la siguiente gráfica.

**Preparatoria**

**Administrativos**

**Empleados**

**Impresoras**

**RB**

**50 hosts**

**1000 hosts**

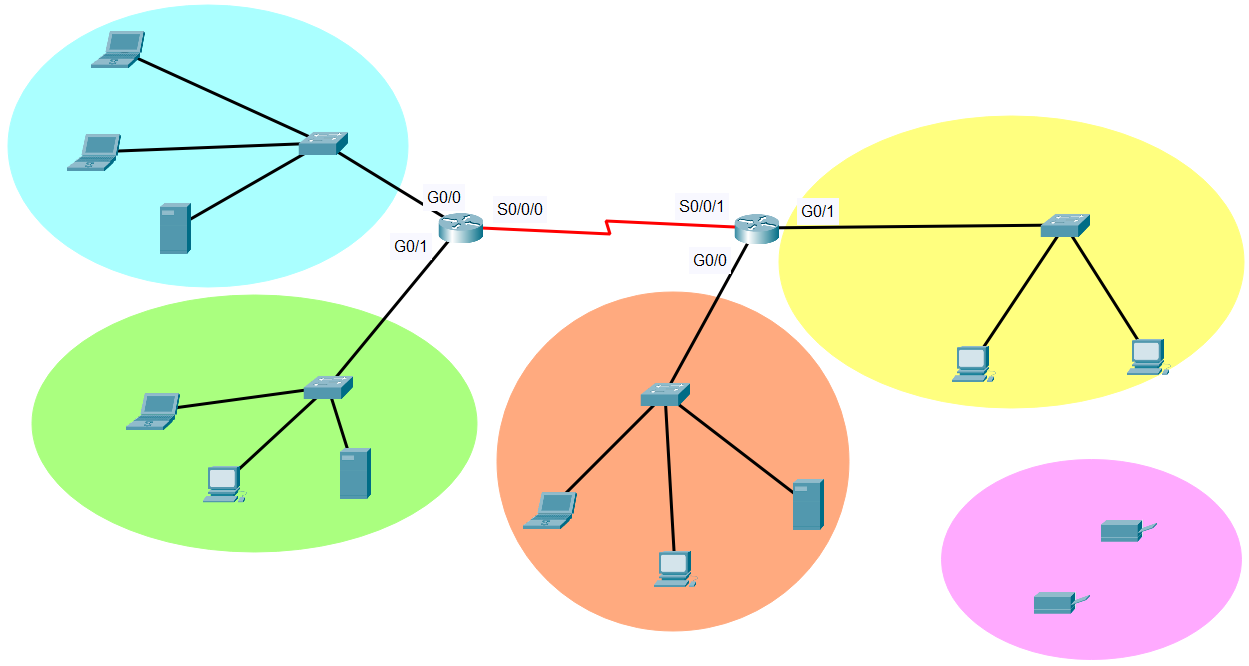
**520 hosts**

**3500 hosts**

**RA**

**Profesional**

**4000 hosts**



1. Utilice la información de la gráfica y diseñe en la tabla el esquema de direccionamiento con máscaras de longitud variable (VLSM). **NOTA:** Tomar en cuenta una dirección extra para la interface del ruteador en la subredes Giga Ethernet. **NOTA:**Las IPs de los host ya incluyen la dirección IP para las interfaces fast ethernet de los ruteadores.

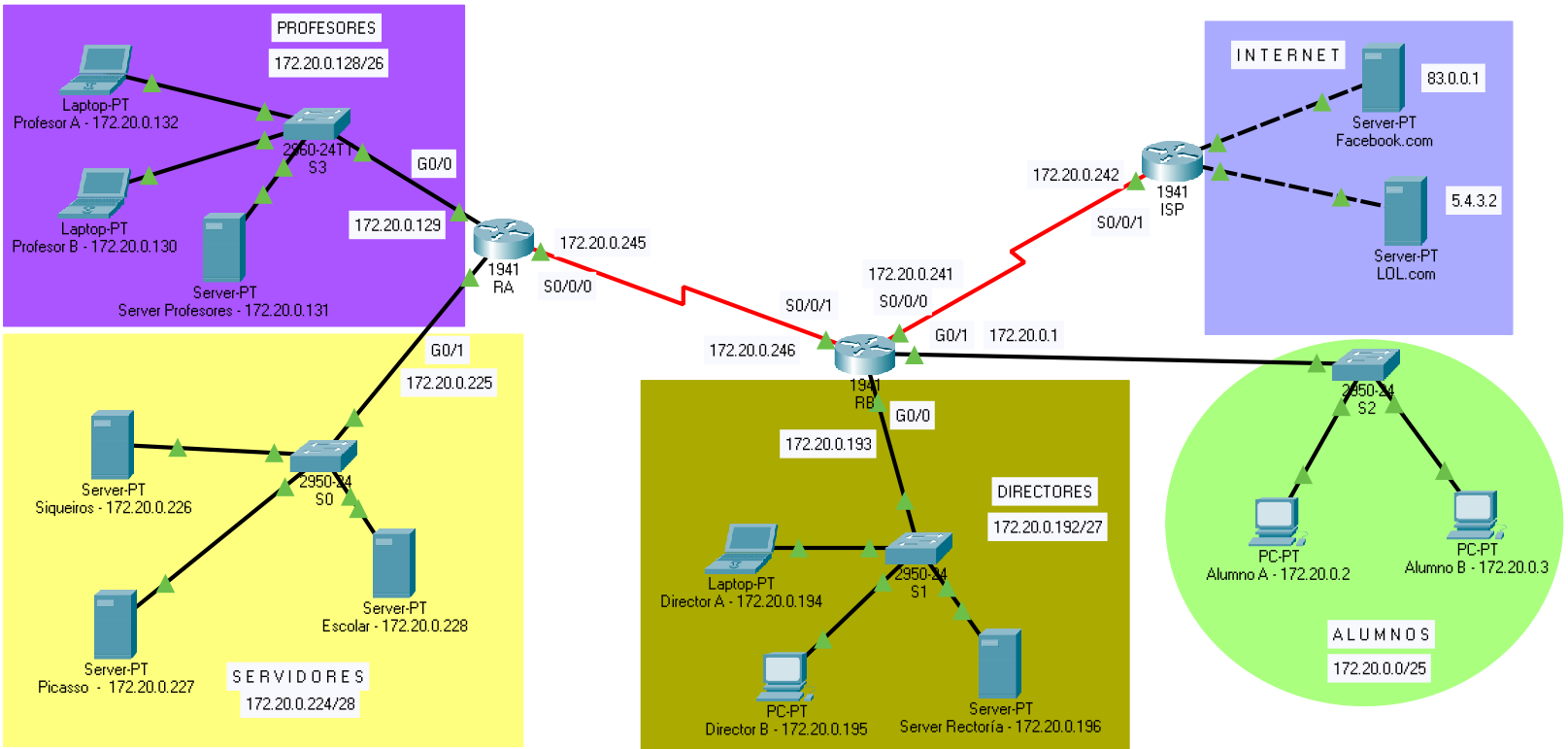
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Descripción**  **Subred** | **Total IPs** | **Bits de host** | **Prefijo de red** | **Máscara en notación decimal** | **Orden** | **Subred** |
| **RA – RB** | 2 | **2 a la 2 – 2 = 2** | **30** | **255.255.255.11111100**  **.252** | **6** | **175.40.232.0** |
| **Profesional** | 4000 | **2ª la 12 = 4096**  **12** | **20** | **255.255.11110000.0**  **255.255.240.0** | **1** | **175.40.192.0**  **. 192+16**  **.208.0**  **192.1 - 207.254 .255** |
| **Administrativos** | 520 | **2 a la 10 – 2 = 1022**  **10** | **22** | **255.255.11111100.0**  **255.255.252.0** | **3** | **175.40.224.0**  **.228.0** |
| **Impresoras** | 50 | 2 a la 6 – 2 =62  6 | **26** | **255.255.255.11000000**  **.192** | **5** | **175.40.232.0**  **.232. 64** |
| **Empleados** | 1000 | **10** | **22** | **255.255.252.0** | **4** | **175.40.228.0**  **.232.0**  **228.1 – 231.255** |
| **Preparatoria** | 3500 | 12 | **20** | **255.255.240.0** | **2** | **175.40.208.0**  **208 + 16**  **224.0** |

1. Realice el diseño de la red y asigne direcciones IP a las interfaces de los routers. Escribe en la siguiente tabla: la IP que será utilizada en cada interface al igual que la máscara de subred, exclusivamente en notación punto decimal.

* Las interfaces **Giga Ethernet** utilizan la **última dirección IP válida** de la subred.
* La interface **s0/0/0** utilizan la **primera dirección IP válida** de la subred.

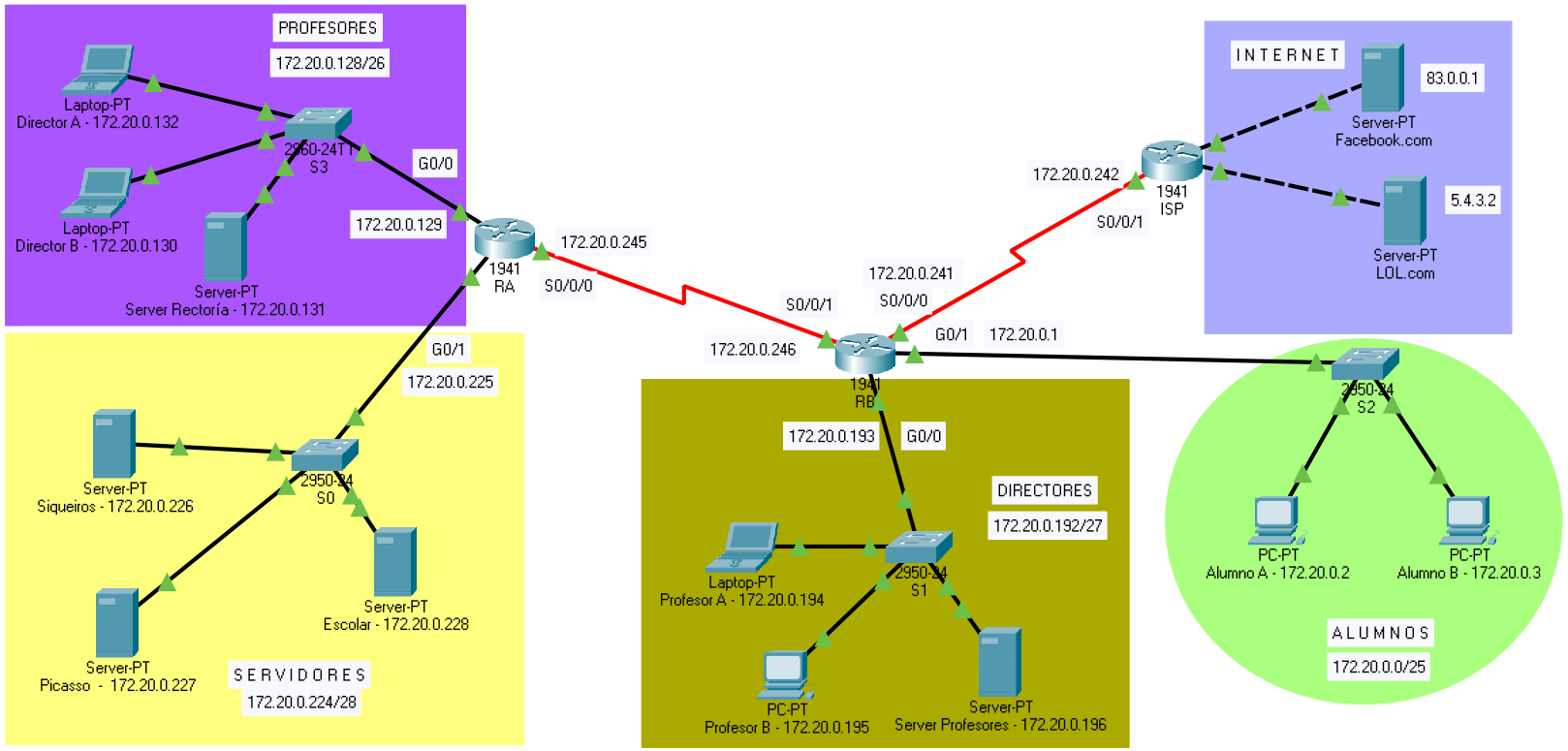
|  |  |  |  |
| --- | --- | --- | --- |
| **Router** | **Interface** | **Dirección IP** | **Máscara de subred** |
| **RA** | **G0/0** | **175.40.207.254** | **255.255.240.0** |
|  | **G0/1** | **175.40.231.254** | **255.255.252.0** |
|  | **S0/0/0** | **175.40.232.1** | **255.255.255.252** |
| **RB** | **G0/0** | **175.40.227.254** | **255.255.252.0** |
|  | **G0/1** | **175.40.223.254** | **255.255.240.0** |
|  | **S0/0/1** | **175.40.232.2** | **255.255.255.252** |

Utiliza la información de la siguiente gráfica y diseña cada una de las listas de control de acceso solicitadas.



Diagrama

Descripción generada automáticamente



**a) Diseña una lista de control de acceso extendida para impedir que cualquier**

**tipo de tráfico que se genere desde una computadora de la subred de Alumnos**

**tenga acceso a cualquier dirección IP de la subred de los Profesores.**

**El tráfico que se generé de otras subredes o que provenga del exterior pasa**

**libremente.**

**NOTA: Esta lista de control de acceso no impide que los Alumnos accedan a**

**los servicios externos de Internet y a los servicios de la subred Servidores**

**y Directores.**

access-list 100 deny ip 172.20.0.0 0.0.0.127 172.20.0.128 0.0.0.63

access-list 100 permit ip any any

RB

int g0/1

ip access-group 100 in

access-list 100 deny ip 132.254.89.0 0.0.0.127 132.254.89.192 0.0.0.31

access-list 100 permit ip any any

!RB

int g0/1

ip access-group 100 in

**b) Diseña una lista de control de acceso que permita que cualquier dirección IP**

**proveniente del exterior tenga acceso exclusivamente al servidor Siqueiros vía el**

**protocolo WEB (exclusivamente el puerto 80). Este servidor estará "oculto"**

**para otro tipo de tráfico que provenga del exterior y que no sea WEB.**

access-list 110 permit tcp any host 172.20.0.226 eq 80

access-list 110 deny ip any host 172.20.0.226

access-list 110 permit ip any any

!RB

int s0/0/0

ip access-group 110 in

**c. Diseña una lista de control de acceso extendida que impida que ninguna dirección IP**

**de la subred de Profesores tengan acceso al servidor de LOL vía el protocolo telnet (23).**

**El resto del tráfico, como web, ftp, ssh, ping, etc.,circula libremente.**

¿Cuál es la lista de control de acceso que permite realizar la acción solicitada?

access-list 120 deny tcp 172.20.0.128 0.0.0.63 host 5.4.3.2 eq 23

access-list 120 permit ip any any

!RA

int g0/1

ip access-group 120 in

**d) Diseña una lista de control de acceso estándar que permita que únicamente las**

**computadoras de la subred de profesores tengan acceso a la subred de Servidores,**

**excepto la computadora del profesor A.**

access-list 1 deny host 172.20.0.132

access-list 1 permit 172.20.0.128 0.0.0.63

ra

int g0/1

ip access-group 1 out

**e) Diseña una lista de control de acceso estándar que permita que únicamente la**

**computadora del Director B tenga acceso a la subred de Servidores.**

access-list 2 permit host 172.20.0.195

ra

int g0/1

ip access-group 2 out

**f) Diseña una lista de control de acceso estándar para impedir que las computadoras**

**de la subred de Directivos tengan acceso a la subred de Profesores.**

access-list 3 deny 172.20.0.192 0.0.0.31

access-list 3 permit any

ra

int g0/0

ip access-group 3 out

**g) Diseña una lista de control de acceso extendida para impedir que las computadoras**

**de la subred de Alumnos tengan acceso a los servidores Siqueiros y Picasso.**

access-list 140 deny ip 172.20.0.0 0.0.0.127 host 172.20.0.226

access-list 140 deny ip 172.20.0.0 0.0.0.127 host 172.20.0.227

access-list 140 permit ip any any

rb

int g0/1

ip access-group 140 in

**h) Diseña una lista de control de acceso extendida que permita únicamente**

**tráfico ssh (22) de la subred de profesores a la subred de servidores.**

access-list 150 permit tcp 172.20.0.128 0.0.0.63 172.20.0.224 0.0.0.15 eq 22

access-list 150 deny ip any any

ra

int g0/0

ip access-group 150 in

i) Diseña una lista de control de acceso extendida que permita únicamente

tráfico ftp (20 y 21) de la subred de alumnos a la subred de profesores.

access-list 160 permit tcp 172.20.0.0 0.0.0.127 172.20.0.128 0.0.0.63 eq 20

access-list 160 permit tcp 172.20.0.0 0.0.0.127 172.20.0.128 0.0.0.63 eq 21

access-list 160 deny ip any any

ra

int g0/1

ip access-group 160 in

**Realiza la migración de la asignación de IPs estáticas a un servicio DHCP**

**4. Instala el servicio dhcp distribuido para las subredes de alumnos, profesores y directivos con el fin de obtener una IP dinámica en cada dispositivo terminal. Excluye las direcciones de los servidores y de las puertas de enlace predeterminadas.**

**En el router RB, diseña y configura los pools de las subredes de Directores y Alumnos.**

**ip dhcp excluded-address 132.54.89.237 132.54.89.238**

**ip dhcp excluded-address 132.54.89.126**

**ip dhcp excluded-address 132.54.89.237 132.54.89.238**

**ip dhcp pool Profesores**

**network 132.254.89.232 255.255.255.248**

**default-router 132.54.89.237**

**ip dhcp pool Alumnos**

**network 132.254.89.0 255.255.255.128**

**default-router 132.54.89.126**

**En el router RA, diseña y configura el pool de la subred de Directores**

**ip dhcp excluded-address 132.54.89.221 132.54.89.222**

**ip dhcp pool Directores**

**network 132.254.89.192 255.255.255.224**

**default-router 132.54.89.222**

**Habilita en cada equipo terminal el servicio de dhcp.**

**Realiza pruebas de conectividad internas y externas.**

**int g0/0**

**ip helper-address 132.254.89.242**

**4. Instala el servicio dhcp centralizado para las subredes de alumnos, profesores y directivos. Excluye las direcciones de los servidores y de las Puertas de enlace predeterminadas.**

**En el router RB, diseña y configura los pools de las subredes de alumnos, profesores y directivos.**

**ip dhcp excluded-address 132.54.89.237 132.54.89.238**

**ip dhcp excluded-address 132.54.89.126**

**ip dhcp excluded-address 132.54.89.221 132.54.89.222**

**ip dhcp pool Profesores**

**network 132.254.89.232 255.255.255.248**

**default-router 132.54.89.237**

**ip dhcp pool Alumnos**

**network 132.254.89.0 255.255.255.128**

**default-router 132.54.89.126**

**ip dhcp pool Directores**

**network 132.254.89.192 255.255.255.224**

**default-router 132.54.89.222**

**En el router RA, configura el ip helper.**

**Habilita en cada equipo terminal el servicio de dhcp.**

**Realiza pruebas de conectividad internas y externas.**

**ip dhcp excluded-address Dir\_IP\_Inicial Dir\_IP\_Final**

**ip dhcp pool NombrePool**

**network dirIP\_inicial Máscara de subred**

**default-router dirIP**

**ip helper-address Dir\_IP**

**Excluir las direcciones de los servidores.**

**Configura dhcp distribuido en cada ruteador.**

**5. Obtener IP dinámica en cada dispositivo terminal.**

**6. Probar conectividad interna y externa.**

**Configuración (Información básica)**

**Bloque amarillo : Home Office**

**192.168.10.0 255.255.255.128**

**default-router 192.168.10.126**

**Bloque entretenimiento : Entretenimiento**

**192.168.10.128 255.255.255.192**

**default-router 192.168.10.190**

**! Vamos a crear el pool para la subred de homeOffice**

**! DHCP para la subred de HomeOffice**

**ip dhcp excluded-address 192.168.10.1 192.168.10.4**

**ip dhcp excluded-address 192.168.10.126**

**! Si las direcciones no son consecutivas tendría**

**! que poner cuatro exclusiones.**

**ip dhcp pool HomeOffice**

**network 192.168.10.0 255.255.255.128**

**default-router 192.168.10.126**

**! DHCP para la subred de Entretenimiento**

**ip dhcp excluded-address 192.168.10.190**

**ip dhcp pool Entretenimiento**

**network 192.168.10.128 255.255.255.192**

**default-router 192.168.10.190**

El gerente regional de TI del Campus Querétaro nos solicita apoyo para ayudar a diseñar esquemas básicos de seguridad que limiten el uso indiscriminado del ancho de banda por aplicaciones ajenas a las académicas.

a) Diseña una lista de control de acceso para impedir que cualquier tipo de tráfico que se genere desde una computadora de la subred de **Alumnos** tenga acceso a cualquier dirección IP de la subred de los **Profesores**. El tráfico que se generé  de otras subredes o que provenga del exterior pasa libremente.

NOTA: Esta lista de control de acceso no impide que los **Alumnos** accedan a los servicios externos de Internet y a los servicios de la subred **Directores y Servidores**.

access-list 100 deny ip 172.20.0.0 0.0.0.127 172.20.0.128 0.0.0.63

access-list 100 permit ip any any

**(8 puntos)**

RB (1 punto)

int g0/1 (2 puntos)

ip access-group 100 in (2 puntos)

router(config)# access-list 10

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**(8 puntos)**

 ¿En qué router asignarás esta lista de control de acceso? \_\_\_\_\_\_\_\_\_\_\_**(3 puntos)**

router(config)# interface \_\_\_\_\_\_\_\_\_ **(2 puntos)**

router(config-if)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **(2 puntos)**

1. El servidor del **ScoreBoard** ha sido instalado en la dirección IP **172.16.1.221**. Diseña una lista de control de acceso que permita que cualquier dirección IP proveniente del exterior tenga acceso exclusivamente al servidor del **ScoreBoard** vía el protocolo **WEB** (exclusivamente el puerto 80). Este servidor estará "oculto" para otro tipo de tráfico que provenga del exterior y  que no sea **WEB**.
2. Diseña una lista de control de acceso que permita que cualquier dirección IP proveniente del exterior tenga acceso exclusivamente al servidor **Siqueiros** vía el protocolo **WEB** (exclusivamente el puerto 80). Este servidor estará "oculto" para otro tipo de tráfico que provenga del exterior y  que no sea **WEB**.

access-list 110 permit tcp any host 172.20.0.226 eq 80

access-list 110 deny tcp any host 172.20.0.226

access-list 110 permit ip any any

**(8 puntos)**

RB (1 punto)

int s0/0/0 (2 puntos)

ip access-group 110 in (2 puntos)

c. Diseña una lista de control de acceso extendida que impida que ninguna dirección IP

de la subred de Profesores tengan acceso al servidor de LOL vía el protocolo telnet (23).

El resto del tráfico, como web, ftp, ssh, ping, etc.,circula libremente.

¿Cuál es la lista de control de acceso que permite realizar la acción solicitada?

access-list 120 deny tcp 172.20.0.128 0.0.0.63 host 5.4.3.2 eq 23

access-list 120 permit ip any any

!RA

int g0/1

ip access-group 120 in

1. Diseña una lista de control de acceso estándar que permita solamente el tráfico de la subred de profesores a la subred de Servidores, excepto del profesor A.
2. da que impida que ninguna dirección IP

de la subred de Profesores tengan acceso al servidor de LOL vía el protocolo telnet (23).

El resto del tráfico, como web, ftp, ssh, ping, etc.,circula libremente.

¿Cuál es la lista de control de acceso que permite realizar la acción solicitada?

access-list 120 deny tcp 172.20.0.128 0.0.0.63 host 5.4.3.2 eq 23

access-list 120 permit ip any any

!RA

int g0/1

ip access-group 120 in

Querétaro tengan acceso a los servidores de LOL y Facebook (ubicados en la dirección IP 111.65.32.1 y 65.0.1.10 respectivamente) vía el protocolo WEB. El resto del tráfico, como FTP ssh telnet ping etc, circula libremente.

¿Cuál es la lista de control de acceso que permite realizar la acción solicitada?

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(13 puntos)

¿En qué router asignarás esta lista de control de acceso? \_\_\_\_\_\_\_\_\_\_\_\_\_ (3 puntos)

router(config)# interface \_\_\_\_\_\_\_\_\_ (2 puntos)

router(config-if)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (2 puntos)

1. Utiliza la aplicación del PacketTracer de CISCO y la siguiente gráfica para realizar:
   1. El diseño de red.
   2. La configuración de cada uno de los routers.
   3. La instalación de un protocolo de ruteo. Tienes la libertad de utilizar los protocolos de enrutamiento: RIPv2, EIGRP, OSPF para tener conectividad en toda la LAN.
   4. La instalación de DHCP en los routers AAA y BBB.
   5. Instalar esquemas básicos de seguridad.



NOTA: No olvides que el ISP ya está configurado.

Utiliza el archivo **EjerRepaso.pkt** para realizar la configuración solicitada. Tu tarea es crear un diseño de red apropiado y realizar las configuraciones para tener comunicación de las direcciones IP privadas hacia Internet.

En esta ocasión la dirección IP a utilizar en nuestro esquema de red es la dirección **221.45.10.0 con prefijo de red /24.**

Para lograr la conectividad, se sugiere proceder con el siguiente orden:

1. Realizar el diseño de red. Utilice la información de la gráfica y diseñe en la tabla el esquema de direccionamiento con máscaras de longitud variable (VLSM). En la gráfica se establecen las restricciones de conectividad.
2. Asignar las direcciones IP a cada una de las interfaces de los routers. **NOTA:** El router ISP ya está configurado.
3. Realizar la configuración de los nombre de los routers: AAA, rFrontera y BBB.
4. Realizar la configuración de las interfaces de los routers: AAA, rFrontera y BBB.
5. Realizar la configuración del protocolo de ruteo: RIPv2, OSPF o EIGRP.
6. Configurar una ruta por default en el router frontera y distribuir la ruta hacia los routers de la LAN. No olvides poner tantas interfaces pasivas como sea necesario.
7. Instalar el servicio de DHCP en cada uno de los routers AAA y BBB para que cada uno de ellos se hagan cargo de la entrega de direcciones IP de cada dispositivo que así lo solicite. (DHCP distribuido)
8. Habilita la opción para que los equipos terminales de cada LAN puedan obtener dirección IP por DHCP.
9. Realizar las pruebas de conectividad necesarias.

Para comprobar tu configuración, realiza un *ping* desde cada una de las PC’s del diseño de red a la interface **LoopBack** definida en el **ISP**. Si el *ping* es exitoso, tu configuración está correcta.

Diseña e instala las siguientes ACLs. Recuerda que para probarlas, debes des-instalar las ACLs previas.

1. Ningún dispositivo de la LAN que depende del router AAA puede acceder a la red del router BBB
2. Ningún dispositivo de la LAN que depende del router BBB puede acceder al server de Youtube vía WEB
3. Ningún dispositivo de la LAN que depende del router AAA puede acceder al server de Youtube vía FTP
4. Ningún dispositivo de la LAN que depende del router BBB puede acceder al server de CNN por ningún protocolo.
5. Utilice la información de la gráfica y diseñe en la tabla el esquema de direccionamiento con máscaras de longitud variable (VLSM). **NOTA:** Tomar en cuenta una dirección extra para la interface del ruteador en la subredes Fast Ethernet.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Descripción**  **Subred** | **# Hosts necesitados** | **Bits de host** | **Prefijo de red** | **Máscara de subred (notación decimal)** | **Orden** | **Subred** |
| **AAA F0/0** | 34 hosts | 2 a la 6 = 64 – 2 = 62  255.255.255.11000000  6 | **/26** | **255.255.255.192** | **1** | **221.45.10.0**  .64 |
| **BBB F0/0** | 56 hosts | 2 a la 6 = 64 – 2 = 62  255.255.255.11000000  6 | **/26** | **255.255.255.192** | **2** | **221.45.10.64**  .128 |
| **AAA – Rfrontera** | 2 hosts | 2 a la 2 =4 – 2 = 2  255.255.255.11111100  2 | **/30** | **255.255.255.252** | **3** | **221.45.10.128**  .132 |
| **RFrontera - BBB** | 2 hosts | 2 a la 2 =4 – 2 = 2  255.255.255.11111100  2 | **/30** | **255.255.255.252** | **4** | **221.45.10.132** |

Completa la tabla con la información que se solicita escribiendo en cada renglón (exclusivamente notación punto decimal) las **direcciones IP** y las **mascaras de subred** de cada una de las interfaces.

* Las interfaces **Fast Ethernet** utilizan la **última dirección IP válida** de la subred.
* Las interfaces **seriales DCE** utilizan la **primera dirección IP válida** de la subred.

|  |  |  |  |
| --- | --- | --- | --- |
| **Router** | **Interface** | **Dirección IP** | **Máscara de subred** |
| **AAA** | **F0/0** | 221.45.10.62 | 255.255.255.192 |
|  | **S0/0/0** | 221.45.10.130 | 255. 255. 255.252 |
| **RFrontera** | **S0/0/0** | 132.254.89.62 | 255.255.255.192 |
|  | **S0/1/0** | 221.45.10.129 | 255. 255. 255.252 |
|  | **S0/0/0** | 221.45.10.133 | 255.255.255.252 |
| **BBB** | **F0/0/0** | 221.45.10.126 | 255.255.255.192 |
|  | **S0/0/0** | 221.45.10.134 | 255.255.255.252 |