1. Diseña una lista de control (10) de acceso estándar que impida que

las computadoras de la subred de Alumnos tengan acceso a la subred

de Servidores.

**Router A**

**access-list 10 deny 132.254.89.0 0.0.0.127**

**access-list 10 permit any**

**int g0/1**

**ip access-group 10 out**

2. Diseña una lista de control de acceso estándar (15) que impida que las

computadoras de la subred de Alumnos tengan acceso a la subred de Profesores.

**Router B**

**access-list 15 deny 132.254.89.0 0.0.0.127**

**access-list 15 permit any**

**int g0/0**

**ip access-group 15 out**

3. Diseña una lista de control de acceso extendida (115) que impida que las

computadoras de la subred de Alumnos, Profesores y Servidores tengan acceso

externo a los servicios de WEB del servidor LOL.com.

El resto de las direcciones IP pueden acceder sin restricción a todos

los servicios de Internet incluyendo todo el tráfico que no sea WEB y

se dirija al servidor de LOL.com

**Router B**

**access-list 115 deny tcp 132.254.89.0 0.0.0.127 host 111.65.32.1 eq 80**

**access-list 115 deny tcp 132.254.89.232 0.0.0.7 host 111.65.32.1 eq 80**

**access-list 115 deny tcp 132.254.89.128 0.0.0.63 host 111.65.32.1 eq 80**

**access-list 115 permit ip any any**

**int s0/0/0**

**ip access-group 115 out**

4. Diseña una lista de control de acceso extendida (120) que únicamente permita el

acceso vía FTP al servidor Escolar desde cualquier IP asociada con la subred

de los profesores y de los Directores pero que impida el acceso a este servidor

vía FTP desde la subred de los Alumnos.

El resto del tráfico pasa libremente (WEB, SMTP, icmp, etc.).

**Router A**

**access-list 130 permit tcp 132.254.89.232 0.0.0.7 host 132.254.89.131 eq 20**

**access-list 130 permit tcp 132.254.89.232 0.0.0.7 host 132.254.89.131 eq 21**

**access-list 130 permit tcp 132.254.89.221 0.0.0.7 host 132.254.89.131 eq 20**

**access-list 130 permit tcp 132.254.89.221 0.0.0.7 host 132.254.89.131 eq 21**

**access-list 130 deny ip 132.254.89.232 0.0.0.7 host 132.254.89.131**

**access-list 130 deny ip 132.254.89.221 0.0.0.7 host 132.254.89.131**

**access-list 130 deny tcp 132.254.89.0 0.0.0.127 host 132.254.89.131 eq 20**

**access-list 130 deny tcp 132.254.89.0 0.0.0.127 host 132.254.89.131 eq 21**

**access-list 130 permit ip any any**

**Router A**

**access-list 130 permit tcp 132.254.89.232 0.0.0.7 host 132.254.89.131 eq 20**

**access-list 130 permit tcp 132.254.89.232 0.0.0.7 host 132.254.89.131 eq 21**

**access-list 130 permit tcp 132.254.89.221 0.0.0.7 host 132.254.89.131 eq 20**

**access-list 130 permit tcp 132.254.89.221 0.0.0.7 host 132.254.89.131 eq 21**

**access-list 130 deny ip 132.254.89.232 0.0.0.7 host 132.254.89.131**

**access-list 130 deny ip 132.254.89.221 0.0.0.7 host 132.254.89.131**

**access-list 130 deny tcp 132.254.89.0 0.0.0.127 host 132.254.89.131 eq 20**

**access-list 130 deny tcp 132.254.89.0 0.0.0.127 host 132.254.89.131 eq 21**

**access-list 130 permit ip 132.254.89.0 0.0.0.127 host 132.254.89.131**

**access-list 130 permit ip any any**

**int g0/1**

**ip access-group 130 out**

**255.255.255.11111000**

**.248**

5. Diseña una lista de control de acceso extendida que únicamente permita el

acceso al servidor Escolar desde cualquier IP asociada con la subred de los

Alumnos y de los Directores pero que impida el acceso a este servidor desde

otras direcciones IP. En está ocasión el servidor de Escolar al no permitir

ningún tipo de tráfico desde direcciones diferentes de Alumnos y Directivos

dará la impresión de que no existe.

**Router A**

**access-list 160 permit ip 132.254.89.0 0.0.0.127 host 132.254.89.131**

**access-list 160 permit ip 132.254.89.192 0.0.0.31 host 132.254.89.131**

**access-list 160 deny ip any host 132.254.89.131**

**access-list 160 permit ip any 132.254.89.128 0.0.0.63**

**int g0/1**

**ip access-group 160 out**