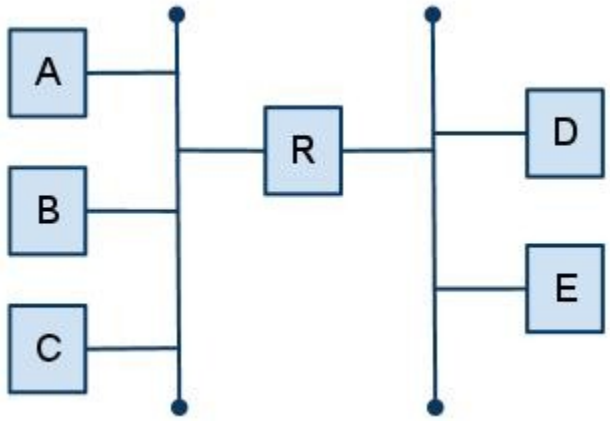
Capa de Aplicación

DNS y Firewall

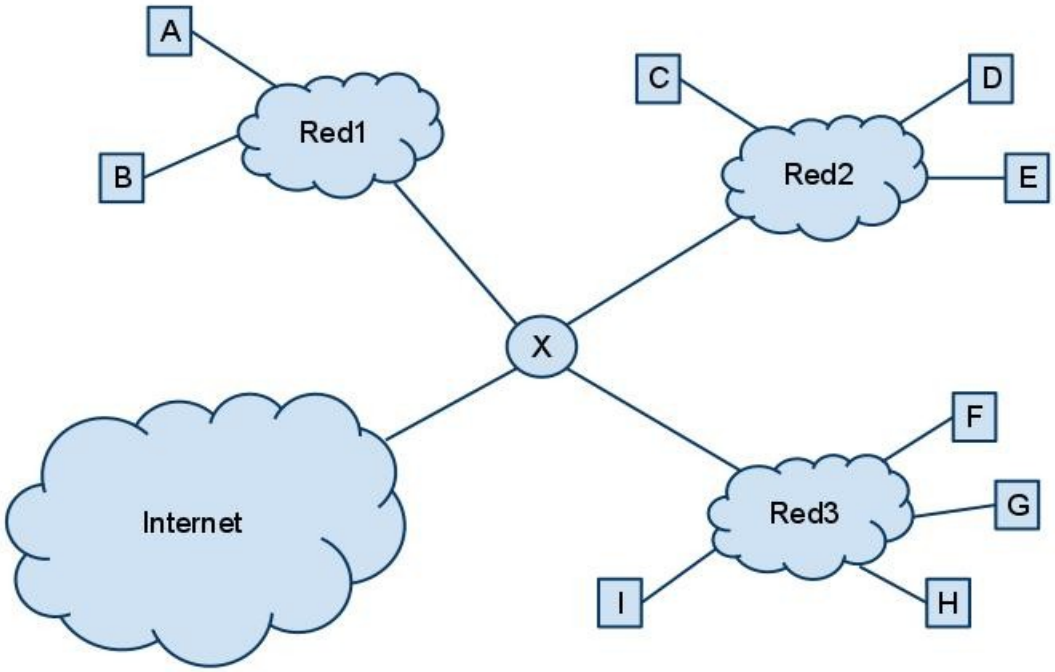
Bibliografía para esta práctica: http://www.zytrax.com/books/dns

1) Dada la red del ejercicio 1) de la Práctica 3 y utilizando las IPs asignadas en su parte c)



   a) Defina un dominio DNS ***ejercicio1.edu.ar.*** para dicha red. y asigne los siguientes recursos:
      i) R servidor DNS maestro autoritativo para ejercicio1.edu.ar. Escriba el archivo de configuración de Bind (llamado *named.conf*) y escriba el archivo de zona para el dominio
      ii) A servidor DNS esclavo. Escriba el archivo de configuración
      iii) B servidor de correo primario
      iv) A servidor de correo secundario
      v) C servidor web y FTP
   b) ¿Qué significa que A sea un servidor DNS esclavo?
   c) ¿Qué significaría que A fuera un servidor DNS secundario?
   d) Agregue al archivo de zona los registros de resolución inversa para el dominio

2) Dada la red del ejercicio 5) de la Práctica 3 y utilizando las IPs asignadas en su apartado c) (es decir que Red1, Red2 y Red3 tienen direcciones privadas RFC 1918):



a) Establezca una **DMZ** en Red3. Configure X como un firewall (escriba la tabla de filtrado con 3 columnas: fuente (IP:puertoTIPO), destino (IP:puertoTIPO) y acción {ALLOW, DENY}) que establezca la política de DMZ en Red3 y además imponga lo siguiente:
   i) Todo anfitrión interno puede acceder libremente a Internet, excepto a servicios SSH en el puerto estándar, a www.youtube.com y tampoco debe acceder a ningún repositorio SVN (sea por cualquiera de los protocolos soportados por SVN: svn://, svn+ssh://, http://, https://)
   ii) Ningún anfitrión de Internet puede iniciar una conexión a un anfitrión interno, sino solo a los siguientes servicios en la DMZ: web, ftp, email, un webservice que corre en un servidor de aplicaciones en el puerto TCP 8080. Los anfitriones de Internet deben ser capaces de acceder esos servicios por su nombre en el sistema DNS.

b) Configure el dominio ***ejercicio4.edu.ar.*** para la red. Cree el archivo de zona DNS con resolución directa e inversa siendo:
   i) A servidor DNS maestro autoritativo para ejercicio4.edu.ar y responde consultas recursivamente para cualquier anfitrión interno para cualquier dominio
   ii) G un servidor DNS esclavo para ejercicio4.edu.ar y responde consultas desde cualquier anfitrión sea interno o de Internet, pero consultas recursivas solamente para anfitriones internos.
   iii) F un servidor de correo primario para ejercicio4.edu.ar
   iv) H un servidor de correo secundario para ejercicio4.edu.ar
   v) H un servidor FTP para ejercicio4.edu.ar
   vi) *client-ejercicio4.webhostingXXX.com.ar* un servidor web para ejercicio4.edu.ar

c) G debe ser capaz de iniciar una transferencia de zona DNS. Asegúrese de que esto es posible. Explique por qué esto viola la política de la DMZ en Red3. Explique cómo se puede mitigar el impacto de esa violación de la política.

d) Se quiere que para el 25 de Mayo el servidor web (www) pase a funcionar en el anfitrión "I" ¿cómo habría que hacer las modificaciones para que hasta el día anterior pueda utilizarse el viejo servidor web?
e) Haga un diagrama de secuencia de paquetes (con direcciones y puertos concretos) intercambiados entre el anfitrión E y el servidor FTP cuando una aplicación en E desea conectarse a *ftp.ejercicio4.edu.ar*. y G es el servidor DNS primario para E
f) Haga un diagrama de secuencia de paquetes (con direcciones y puertos concretos) intercambiados entre un anfitrión en Internet P y el servidor FTP cuando una aplicación en P desea conectarse a *ftp.ejercicio4.edu.ar*.
g) En ambos apartados e) y f), suponiendo que no haya cachés DNS ni direcciones de hosts *hardcodeadas*, en algún momento del intercambio de paquetes, el servidor G respondió una consulta DNS devolviendo un registro de tipo AA con una dirección IP ¿cuál fue esa dirección? ¿en ambos fue la misma? ¿fue exitosa la comunicación en ambos apartados?
h) Solucione el problema del apartado g) re-escribiendo el archivo de zona usando la cláusula *view* de Bind[1].

3) Con las mismas IPs y servidores que en el punto 2) anterior, configure el subdominio *intra.ejercicio4.edu.ar* y **delegue** la autoridad sobre el mismo a los siguientes servidores DNS
   a) A será maestro autoritativo para intra.ejercicio4.edu.ar. Modifique el named.conf (elija la configuración más adecuada) y el archivo de zona *ejercicio4.edu.ar* y escriba un nuevo archivo de zona para *intra.ejercicio4.edu.ar*.
   b) D servidor DNS esclavo del anterior y autoritativo para la zona *intra.ejercicio4.edu.ar*. Escriba el named.conf

1 "DNS Bind view Clause", capítulo 7 del libro de zytrax.