

ADMINISTRACIÓN Y CONFIGURACIÓN DE REDES (EIMT1019) - CURSO 2018-2019

BOLETÍN DE PROBLEMAS P7

NOMBRE Y APELLIDOS:

GRUPO (PR1/PR2/PR3):

FIRMA

.....

INTRODUCCIÓN.

Una de las herramientas que pueden utilizarse para aportar seguridad de una red es el uso de listas de control de acceso (ACL). En ellas se definen las reglas que pueden prevenir el tráfico de algunos paquetes a través de la red. Se pueden utilizar ACLs IP numeradas o estándares (se especifica IP de origen) o ACLs IP extendidas (se especifica varios parámetros, IP de origen y destino o puertos de origen y destino). En los siguientes ejercicios vamos a utilizar la configuración de red de la figura 1.

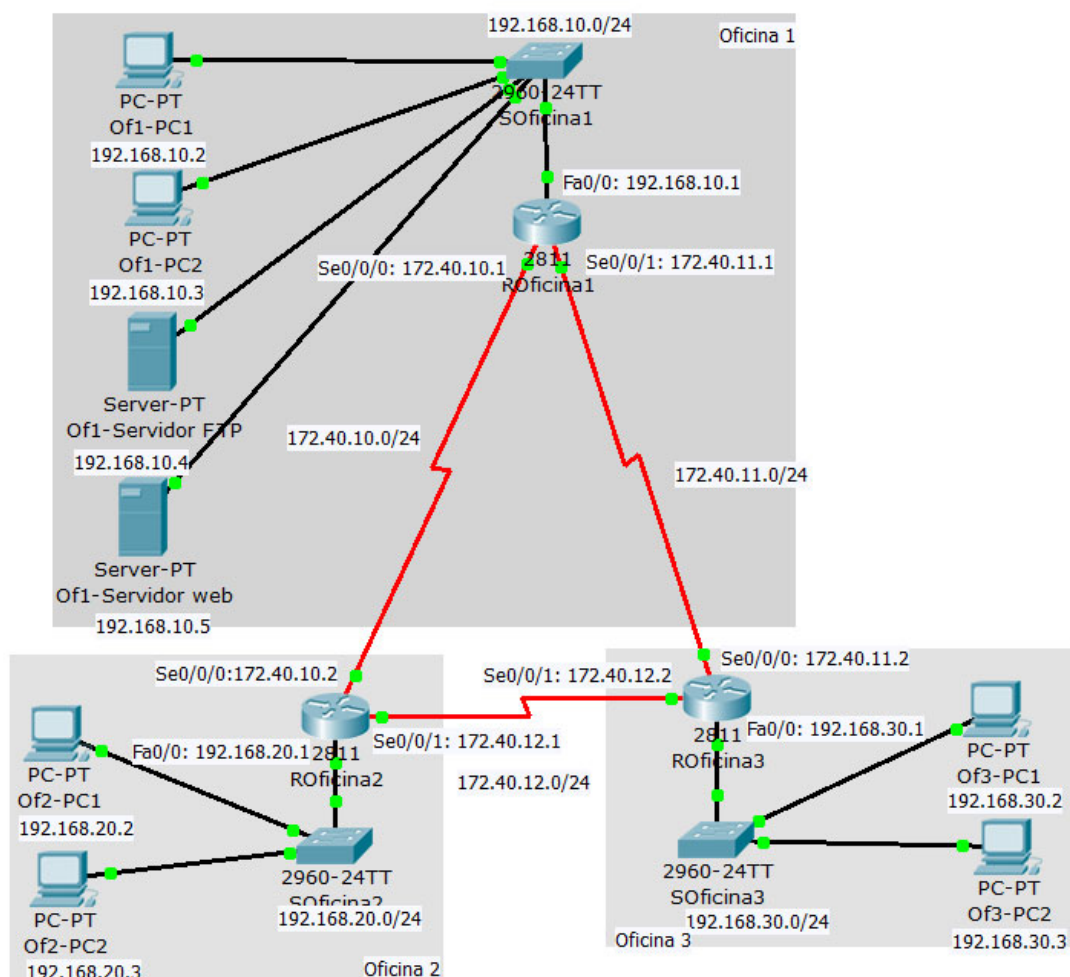


Figura 1. Configuración de la red.

LISTAS DE ACCESO ESTÁNDARES

EJERCICIO 1. Configuración de listas de control de acceso IP estándares.

Con la configuración inicial que aparece en la Figura 1, genera en el Router adecuado la ACL estándar necesaria para que **el Of1-PC2 no pueda salir de Oficina 1 y el resto de tráfico esté permitido.**

- 1) Indica el router en donde crearás la lista y la interfaz o interfaces del mismo en donde aplicar la lista.
- 2) Crear un comentario con la opción “*access-list 10 remark*” que indique en la ACL “**el Of1-PC2 no pueda salir de Oficina 1**”. Escribe también los comandos necesarios para genera la lista ACL con número 10 que cumplan los requisitos que el tráfico de PC Of1-PC2 no pueda salir de Oficina1 y el resto de tráfico está permitido.
- 3) Indica los comandos para aplica la ACL en las interfaces que diste en el apartado 1). Indica primero el router (por ejemplo: “ROficinaX:”) y después escribe los comandos para aplicar la lista en la o las interfaces adecuados del router.
- 4) ¿Crees que con la lista creada un PC de la Oficina 3 podrá acceder al Of1-PC2? Justifica tu respuesta.

LISTAS DE ACCESO EXTENDIDAS

EJERCICIO 2

Cuando necesitamos filtrar tráfico entre direcciones IP (o puertos de protocolos) de origen y destino será necesario el uso de listas de control de acceso extendidas.

Configuración de ACLs IP extendidas para denegar tráfico entre 2 host.

Con la configuración inicial que aparece en la Figura 1 genera las ACLs extendidas necesarias para que **el pc Of1-PC2 no pueda acceder al pc Of3-PC1 y el resto de tráfico será permitido.** Veamos los pasos a seguir:

- 5) ¿Cuál será el Router adecuado para aplicarle las listas?
- 6) Crear un comentario con la opción “*access-list 101 remark*” que indique en la ACL “**Of1-PC2 no pueda acceder a Of3-PC1**”. Escribe también los comandos necesarios para genera la lista ACL con número 101 que cumplan los requisitos que el tráfico de Of1-PC2 no pueda acceder al pc Of3-PC1 y el resto de tráfico esté permitido.
- 7) Indica los comandos para aplica la lista en la o las interfaces adecuadas del router que indicaste en 5).

EJERCICIO 3

Configuración de ACLs IP extendidas para denegar tráfico entre dos redes.

Con la configuración inicial que aparece en la Figura 1, genera en el Router adecuado las ACLs extendidas necesarias para que **los hosts de Oficina 2 no puedan acceder a los host de Oficina 3 y el resto de tráfico esté permitido.** Pasos a seguir:

- 8) ¿Cuál será el Router adecuado para aplicarle las listas?

- 9) Crear un comentario con la opción “*access-list 102 remark*” que indique “**los hosts de Oficina 2 no pueden acceder a los host de Oficina 3 y el resto de tráfico está permitido**”. Escribe también los comandos para crear la ACL con número 102 que cumpla los requisitos **los hosts de Oficina 2 no puedan acceder a los host de Oficina 3 y el resto de tráfico esté permitido.**

- 10) Indica los comandos para aplica en la interfaz adecuada la lista de acceso creada.

- 11) ¿Con esta lista un PC de la oficina 3 podrá alcanzar a un PC de la oficina 2? Justifica tu respuesta.

EJERCICIO 4

Configuración de listas de control de acceso IP extendidas para denegar tráfico especificando protocolos y puertos de origen y/o destino.

Con la configuración inicial que aparece en la Figura 1, queremos generar en el Router adecuado una ACL extendidas para que:

- el pc Of3-PC1 no pueda acceder al pc Of1-PC2,*
- denegar el tráfico FTP de Of3-PC1 al servidor ftp en oficina1*
- denegar el tráfico HTTP de Of3-PC2 al servidor web en oficina1*
- que el resto de tráfico esté permitido.*

12) Indica en que router e interfaces del mismo lo aplicarías y los comandos para hacerlo.

13) Escribe los comandos para generar la ACL 110 con los requisitos anteriores.