GII TDRC
Práctica 5
Seguridad en Acceso y distribución

Duración: 1 sesion

Objetivos	El objetivo de esta práctica es la interiorización por parte de los alumnos de los conceptos teóricos relacionados con seguridad en switches de acceso y listas de acceso en routers de distribución.
Conocimientos previos	Para el aprovechamiento de esta práctica se necesitan los siguientes conocimientos adquiridos en las clases teóricas y seminarios: • Comandos básicos de configuración equipos Cisco • Comandos de configuración y diagnóstico de Mac seguras y monitorización de puertos • Comandos de configuración y diagnóstico de listas de acceso
IMPORTANTE!!	• Los accesos a los equipos se harán a través de la red de Gestión. • La práctica se realizan en grupo por ISLAS. En cada isla habrá al menos 2 parejas, de modo que cada pareja se encargue de configurar uno de los 2 routers y switchs de la isla (Rx_A, Swx_A y Rx_B, SWx_B) • La práctica hay que resolverla a nivel de Isla. Antes preguntar cualquier duda al profesor, ésta debe ser tratada previamente entre todos los miembros de la isla. En cada isla se elegirá un delegado que será la única persona autorizada para preguntar/resolver dudas con el profesor. • Para la evaluación final se tomará a un alumno por isla que tendrá que completar una serie de tareas. Es responsabilidad de la propia isla que todos sus miembros sean capaces de completar la práctica con éxito. Este alumno no será en ningún caso el delegado de la isla. • Al final de la práctica existe un ANEXO I con algunos nuevos comandos así como un plano de topología que deberá completar en el ANEXO II. El Anexo III incluye ejemplos de configuraciones vistos en clase.

1.- Configuración PC	1. Inicie su PC desde **Red Aislada, Windows XP Redes** 2. Acceda como administrador (usuario**: root;** password**: finisterre**). 3. Anote la isla y PC (vea la etiqueta encima del PC) **ISLA:** **PC:** 4. En cada isla **x**, cada PC trabajará con la red de gestión, que será usada para poder hacer telnet a los routers. También trabajará con tan solo una de las redes de Servicios y desactivará la otra. **PCx/1, PCx/2: Desactivan interfaces de Servicios B** **PCx/3, PCx/4: Desactivan interfaces de Servicios A** Desactivación de interfaz: Inicio-Panel de control-Conexiones de red—

Servicios. Situarse sobre la red a desactivar, botón derecho-desactivar

5. Se comprueba que la red correspondiente a quedado desactivada mediante el comando **ipconfig.**
6. A continuación se asigna a cada PC el default gateway de la red de Servicios con la que va a trabajar (la que no se ha desactivado), que será

   PCx/1, PCx/2: Default Gateway 10.x.1.100
   PCx/3, PCx/4: Default Gateway 10.x.2.100

Configuración Default Gateway: Inicio-Panel de control-Conexiones de red—Servicios. Situarse sobre la red de servicios activa, hacer -doble-click-Propiedades-ProtocoloTCP/IP-Puerta de enlace predeterminada.

7. Se comprueba que el PC ha tomado el Default Gateway mediante el comando **ipconfig.**
8. Rellene sobre el plano de topología del ANEXO II, los valores de direccionamiento IP de PC1-PC4 en su isla

2.- Configuración de rutas estáticas

Objetivo: En este apartado tendrá que configurar rutas estáticas en Rx_A y Rx_B para poder llegar a las Redes de Servicios B y A respectivamente a través de la Red de Gestión.

9. Para cada router tenemos
   usuario: **laboratorio**, password: **telemática**

10. Observe el plano de Topología del ANEXO II. Los next-hops que se usarán en las rutas estáticas serán las direcciones IP de los interfaces F0/1 de Rx_A y Rx_B.

11. Configure las rutas estáticas en Rx_A y Rx_B para poder llegar a las redes de servicios B y A respectivamente

    Ip route <red destino> <máscara> <next-hop>

12. Compruebe que existe conectividad entre las Redes de Servicios A y B a través de la Red de Gestión. Para ello haga y **traceroute** desde PC1 a PC4 y desde PC3 a PC2.

13. Sobre el ANEXO II, rellene toda la información que se indica.

    - Para cada PC: Dirección IP, máscara, DG y MAC.
    - Para RX_a y RX_B: direcciones IP de F0/0/0 y F0/1
    - Para SWx_A y SWx_B: Puertos de acceso a los PCs y routers

CUANDO TODAS LAS PAREJAS DE LA ISLA HAYAN LLEGADO A ESTE PUNTO AVISE AL PROFESOR Y ESPERE ANTES DE CONTINUAR

3.- Seguridad a nivel de aceso: Monitorización de puertos

OBJETIVO: La tarea consigue en que el PCx/1 monitorice el tráfico icmp generado mediante ping entre PCx/2 y RxA (lo mismo para PCx/3 con PCx/4 y RxB).

IMPORTANTE: Antes de hacer nada, lea completamente este apartado e interiorice los pasos que hay que completar. De esta forma tendrá la visión necesaria para entenderla en su globalidad. Antes de empezar, el delegado de cada isla deberá reunir a todos los miembros en una reunión para aclarar todas las dudas posibles de los miembros de la isla.

- Ejecute Wireshark en PCx/2 y PCx/4 sobre el interfaz de la red de Servicios A y B respectivamente.
- Ejecute desde PCx/2 y PCx/4 un **ping continuo** contra el interfaz F0/0/0 del router RxA y RxB respectivamente y compruébelo tanto en la ventana de comandos de Windows (cmd) como en Wireshark.
- Ejecute Wireshark en PCx/1 y PCx/3 sobre el interfaz de la red de Servicios A y B respectivamente y responda
    - ¿Es capaz de observar el ping continuo entre PCx/2 y PCx/4 y RxA y RxB? ¿Por qué?

- Siguiendo el ejemplo del ANEXO III, habrá que configurar un **monitor** en el puerto de los switches SWxA y SWxB en el que están conectados PCx/1 y PCx/3 respectivamente. Desde este puerto **monotorizaremos** el puerto de PCx/2 y PCx/4 respectivamnte.
- Reúnanse los 4 miembros de la isla y escriban a continuación los comandos que habría que escribir en cada Switch. Coteje los comandos de monitorización de puertos del ANEXO I antes de rellenar la tabla y el ejemplo del ANEXO III.

SWxA	
SWxB	

CUANDO TODAS LAS PAREJAS DE LA ISLA HAYAN LLEGADO A ESTE PUNTO AVISE AL PROFESOR Y ESPERE ANTES DE CONTINUAR

- Antes de configurar los comandos de la tabla anterior, deber borrar configuraciones previas de seguridad que haya en el switch. Para ello borre en el interfaz que quiere configurar, cualquier línea que empiece por

  switchport port-security ….

- Introduzca los comandos de la tabla anterior

- Compruebe en ahora Wireshark sí presenta en PCx/1 y PCx/3 el **ping continuo** de PCx/2 y PCx/4.

CUANDO TODAS LAS PAREJAS DE LA ISLA HAYAN LLEGADO A ESTE PUNTO AVISE AL PROFESOR Y ESPERE ANTES DE CONTINUAR

4.- Seguridad a nivel de aceso: MAC seguras (opcional)

OBJETIVO: La tarea consigue en asegurar el puerto de acceso de cada PC al switch mediante el uso de MAC seguras en modo estático. La acción a ejecutar en caso de violación de MAC será shutdown del puerto.

IMPORTANTE: Antes de hacer nada, lea completamente este apartado e interiorice los pasos que hay que completar. De esta forma tendrá la visión necesaria para entenderla en su globalidad. Después, el delegado de cada isla deberá reunir a todos los miembros en una reunión para aclarar todas las dudas posibles de los miembros de la isla.

- Para cada PC, averigüe la MAC de su Interfaz de Servicios y anótela en la siguiente tabla. También anótela en la topología del ANEXO II si no lo hizo previamente.

PC	Red de Servicios A/B	MAC
PCx/1	**A**	
PCx/2	**A**	
PCx/3	**B**	
PCx/4	**B**	

- Coteje los comandos de seguridad de puertos del ANEXO I antes de rellenar la tabla y el ejemplo del ANEXO III. Todos los alumnos de la isla deben reunirse y escribir en la siguiente tabla los comandos necesarios para configurar el objetivo de la práctica. NO INTRODUZCA POR AHORA NINGUN COMANDO EN EL SWITCH

SWxA	
SWxB	

CUANDO TODAS LAS PAREJAS DE LA ISLA HAYAN LLEGADO A ESTE PUNTO AVISE AL PROFESOR Y ESPERE ANTES DE CONTINUAR

- Antes de configurar los comandos de la tabla anterior, deber borrar configuraciones previas de seguridad que haya en el switch. Para ello borre en el interfaz que quiere configurar, cualquier línea que empiece por

  switchport port-security ….

- Configure los comandos de la tabla anterior

- Compruebe que los PCs de la isla tiene conectividad entre sí. Para ello realice un **ping continuo** entre PCx/1->PCx/2 y PCx/3->PCx4.

- Para provocar una violoación de MAC, intercambiaremos entre sí los cables de red de los interfaces de la red de Servicios

  PCx/1<—>PCx/2 en el SWxA
  PCx/3<—>PCx/4 en el SWxB.

  Para ello pida a su profesor que le abra el rack para hacer el cambio de cables. ESTO SE REALIZARA PARA TODOS LOS MIEMBROS DE LA ISLA AL MISMO TIEMPO. LA ACCIÓN LA REALIZARÁ EL DELEGADO DE LA ISLA EN PRESENCIA DE TODOS LOS MIEMBROS.
  - ¿Qué es lo que se pretende causar en los switches?

- Compruebe que se ha provocado un **shutdown** del puerto (luz roja en el puerto o ausencia de luz según versiones) en SWxA y SWxB al detectar que la MAC con la que llegan las tramas del **ping continuo** no es la correspondiente a la MAC segura de esos puertos.

- Conéctese a su switch mediante el interfaz de la red de gestión y compruebe qué puertos están en modo shutdown (**show ip interface brief**)

  - ¿Coinciden estos puertos con los puertos en los que se produjo violación de MAC?

- Vuelva al estado normal antes de la violación de MAC, para ello
    - Vuelva a conectar cada cable en su sitio (LO HARÁ EL DELEGADO DE LA ISLA EN PRESENCIA DE TODOS LOS MIEMBROS)
    - Vuelva a activar en el switch todos los puertos que estaban en modo shutdown. Para ello ejecute, en cada puerto los comandos

      shutdown
      no shutdown
    - Compruebe que el **ping continuo** se recuepra automáticamente

CUANDO LLEGUE A ESTE PUNTO AVISE AL PROFESOR Y ESPERE ANTES DE CONTINUAR

5.- Seguridad a nivel de distribución:

Listas de acceso

OBJETIVO: La tarea consigue en configurar una serie listas de acceso extendidas en los routers RxA y RxB que limiten la conectividad

IMPORTANTE: Antes de hacer nada, lea completamente este apartado e interiorice los pasos que hay que completar. De esta forma tendrá la visión necesaria para entenderla en su globalidad. Antes de empezar, el delegado de cada isla deberá reunir a todos los miembros en una reunión para aclarar todas las dudas posibles de los miembros de la isla.

- Fijándose en los ejemplos del ANEXO III, el delegado de cada isla debe reunir a todos los miembros para escribir la configuración de las siguientes listas de acceso. no introduzca por ahora ningun comando en el router.

  PRIMERA LISTA DE ACCESO

1. Que ningún host de la subred de Servicio A donde está PCx/1 pueda hacer ping a ningún host de la subred de Servicios B en la que está PCx/3. Que permita el resto de tráfico.

RxA	
RxB	

SEGUNDA LISTA DE ACCESO

- Que al RxA solo le pueda hacer telnet los hosts PCx/1 y PCx/2 por cualquiera de sus interfaces. Que al RxB solo le pueda hacer telnet los hosts PCx/3 y PCx/4 por cualquiera de sus interfaces. Que permita el resto de tráfico.

RxA	
RxB	

CUANDO LLEGUE A ESTE PUNTO AVISE AL PROFESOR Y ESPERE ANTES DE CONTINUAR

- **IMPORTANTE**: Para evitar interferencias con prácticas anteriores en las que se configuraron los **switches**, antes de empezar la práctica, borre todos los comandos introducidos en ellos.

- Antes de introducir las listas de acceso compruebe que:
  - Que cualquier host de la subred de Servicios A donde está PCx/1 pueda hacer ping a cualquier host de la subred de Servicios B en la que está PCx/3.
  - Que tanto al RxA como al RxB le pueden hacer telnet hosts cualquier host de cualquier red.
- Configure los comandos de la PRIMERA LISTA DE ACCESO y compruebe SU EFECTO
- Configure los comandos de la SEGUNDA LISTA DE ACCESO y compruebe SU EFECTO

CUANDO TODAS LAS PAREJAS DE LA ISLA HAYAN LLEGADO A ESTE PUNTO AVISE AL PROFESOR Y ESPERE ANTES DE CONTINUAR

Anexo I

Lista de comandos Cisco

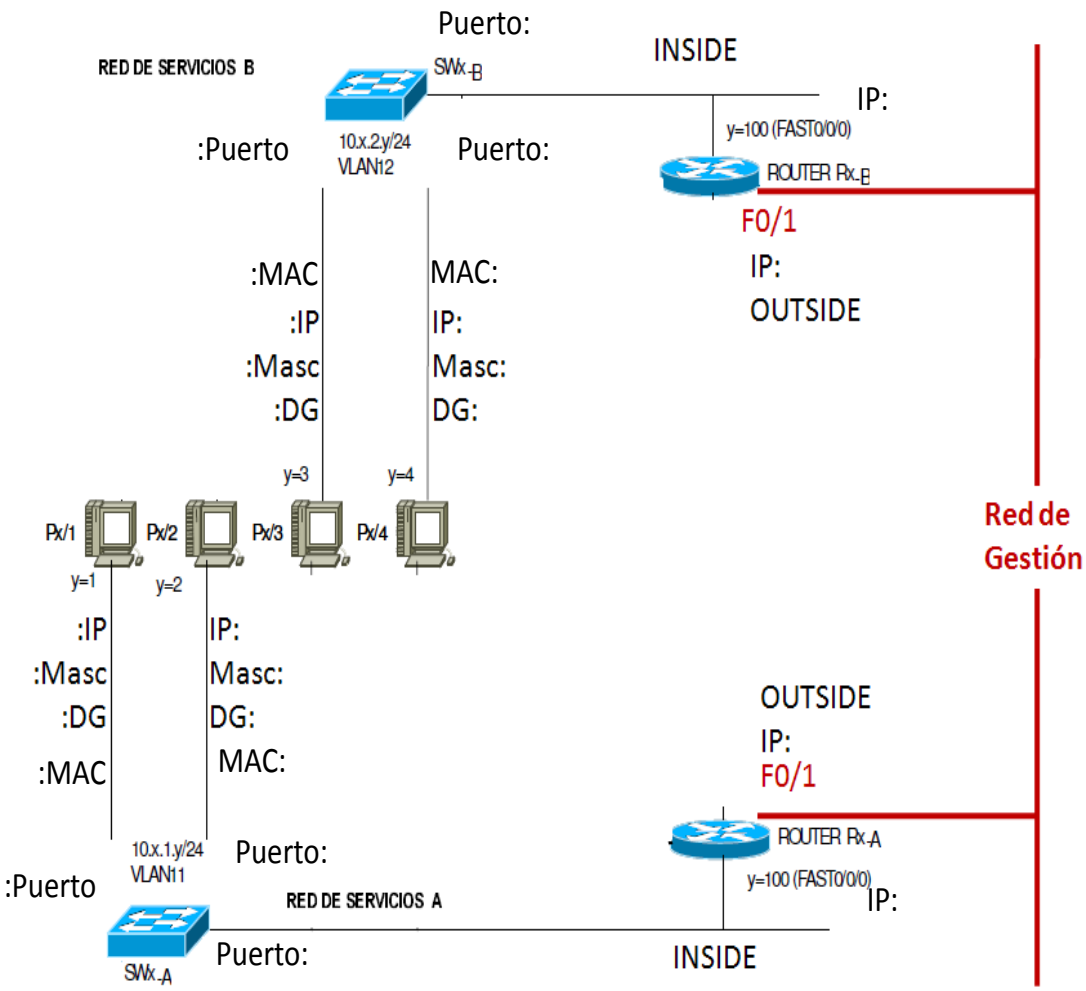
Comandos de monitorización de puertos
monitor session 1 source interface <interfaz que es monitorizado>
monitor session 1 destination interface <interfaz que monitoriza>

Comandos Seguridad en puertos
switchport -por security
switchport -por security mac-address
switchport -por security violation
switchport -por security maximum
show port address

Comandos de listas de acceso
access-list <number 100..199> [permit | deny] [tcp | ip | icmp] ...
ip access-group <number 100..199> [out | in]
show access-list

ANEXO II PLANO TOPOLÓGICO

NOTA: Por claridad, los interfaces de los Pcs a la red de Gestión no están indicados en la figura.



ANEXO III.

CONFIGURACIÓN MONITORIZACIÓN DE PUERTOS

Ejemplo para los switches 2900/3500**:**

• Ejemplos de configuración

2900XL/3500XL SPAN
Ejemplo de Configuracion

```
interface FastEthernet0/1
 port monitor FastEthernet0/2
 port monitor FastEthernet0/5
 port monitor VLAN1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
 switchport access vlan 2
!
```

```
!
interface FastEthernet0/4
 port monitor FastEthernet0/3
 port monitor FastEthernet0/6
 switchport access vlan 2
!
interface FastEthernet0/5
!
interface FastEthernet0/6
 switchport access vlan 2
!
```

Ejemplo para los switches 2950:

La monitorización de puertos se realiza a nivel de configuración global.
(config)# monitor session 1 source interface <interfaz que es monitorizado>
(config)# monitor session 1 destination interface <interfaz que monitoriza>

CONFIGURACIÓN MAC SEGURA ESTÁTICA

Ejemplo incompleto

• Ejemplos de configuración

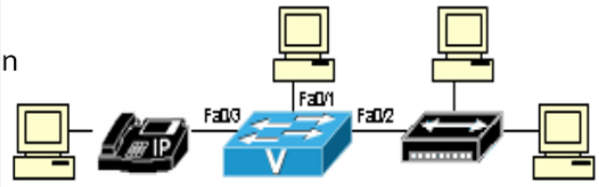


Figure 1. Example Network

Example of a Static Secure MAC Address:

```
Switch#configure terminal
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address 0000.0102.0304
Switch(config-if)#end
```

CONFIGURACIÓN LISTA DE ACCESO EXTENDIDA

• Ejemplos de aplicación: Extendida