



#### **2.4.7: Configuración de la administración básica del switch**



**Alumno:** Miguel Santiago Cervilla

**Profesor:** Julián García Donaire

**Integración de las Tecnologías de la Información en las Organizaciones**

**Grado Ingeniería Informática**

**Curso 2018/19**

**1**

# Índice

1. Introducción	3
2. Resolución actividad	4-11
3. Conclusiones	12
4. Bibliografía.	13

**Alumno:** Miguel Santiago Cervilla

**Profesor:** Julián García Donaire

**Integración de las Tecnologías de la Información en las Organizaciones**

**Grado Ingeniería Informática**

**Curso 2018/19**

# 1. Introducción

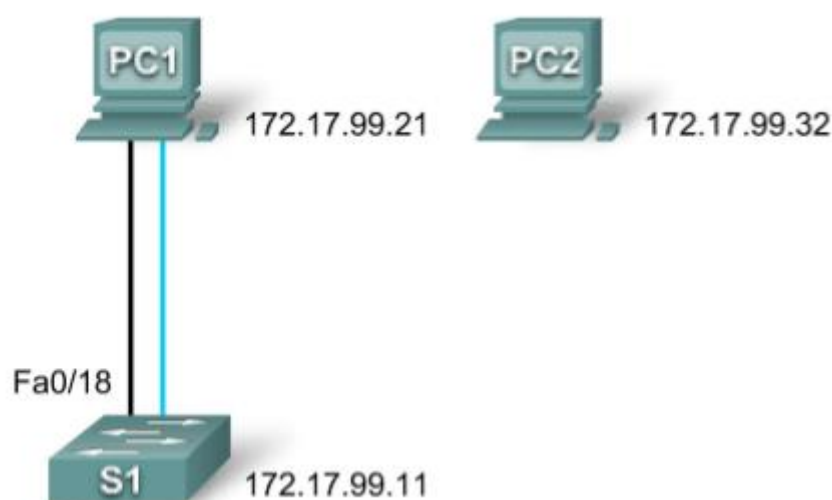


Figura 1. Diagrama de topología

Dada la topología de la **Figura 1** vamos a practicar con al creación de VLAN.

La administración básica del switch es la base de la configuración de los switches. Esta actividad se centra en la navegación entre los modos de interfaz de la línea de comandos, el uso de las funciones de ayuda, el acceso al historial de comandos, la configuración de parámetros de la secuencia de arranque, la definición de la configuración de velocidad y duplex; además de la administración de la tabla de direcciones MAC y el archivo de configuración de switch. Las habilidades adquiridas en esta actividad son necesarias para la configuración de la seguridad básica del switch incluida en capítulos posteriores.

Se nos proporciona la tabla de direcciones siguiente:

Dispositivo	Interfaz	Dirección IP	Máscara subred
<b>S1</b>	<b>VLAN99</b>	172.17.99.11	255.255.255.0
<b>PC1</b>	<b>NIC</b>	172.17.99.21	255.255.255.0
<b>Server</b>	<b>NIC</b>	172.17.99.31	255.255.255.0

Tabla 1. Tabla de direcciones.

**Alumno:** Miguel Santiago Cervilla

**Profesor:** Julián García Donaire

Integración de las Tecnologías de la Información en las Organizaciones

Grado Ingeniería Informática

Curso 2018/19

3

## 2. Resolución actividad

**Paso 1: Desde PC1, acceda a la conexión de consola a S1.**

Primer paso, nos conectaremos al switch:

- Utilizamos un cable de consola y conecte la interfaz RS 232 de PC1 a la interfaz de la consola del switch S1.
- Hacemos clic en PC1 y luego en la ficha Desktop. Seleccionamos Terminal de la ficha Desktop.
- Conservaremos la configuración por defecto para la Terminal Configuration, y luego haga clic en OK. Bits Per Second = 9600 Data Bits = 8 Parity = None Stop Bits = 1 Flow Control = None
- El usuario está conectado a la consola en S1. Presione Intro para ver el indicador Switch.

Una vez realizado lo anterior, vamos a navegar por los modos CLI. Para ello vamos a seguir los siguientes pasos y los **vamos a mostrar con capturas de pantalla** de los pasos que se realizan:

**Paso 2: Cambie al Modo EXEC privilegiado.**

```
Switch>  
Switch>enable  
Switch#
```

Figura 2. Modo privilegiado

Como podemos observar en la **Figura 3**, hemos entrado en modo **EXEC**.

Contestaremos a la siguiente cuestión:

**¿Por qué la ausencia de una contraseña para el Modo EXEC privilegiado constituye una amenaza de seguridad?**

Constituye una amenaza de seguridad, ya que cualquier usuario podría acceder a la configuración interna sin ningún tipo de restricción.

### Paso 3: Cambie al modo de configuración global y configurar la contraseña EXEC privilegiado.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

Figura 3. Configuración global

```
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#enable secret class
S1(config)#
```

Figura 4. Cambio de contraseña

### Paso 4: Configure contraseñas de terminal virtual y de consola e introducir el comando login.

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

Figura 5. Cambio contraseña virtual y contraseña de consola

### Paso 5: Configure la encriptación de contraseñas.

Usamos el comando **service password-encryption**

```
S1(config)#service password-encryption
S1(config)#
```

Figura 6. Encriptación contraseñas

### Paso 6: Configure y probar el mensaje MOTD.

Configuramos un mensaje con el comando **MOTD**

```
S1(config)#banner motd &Authorized Access Only&
S1(config)#end [o exit]
S1#exit
```

Figura 7. Configurar MOTD

Una vez realizados los pasos anteriores, vamos a seguir con una nueva serie de pasos a completar para realizar la actividad.

**Alumno:** Miguel Santiago Cervilla

**Profesor:** Julián García Donaire

Integración de las Tecnologías de la Información en las Organizaciones

Son los siguientes:

### Paso 1: Habilite VLAN99.

Vamos a habilitar la interfaz VLAN 99 con el comando **no shutdown**

```
S1(config)#interface vlan 99
S1(config-if)#no shutdown
```

Figura 8. Habilidad interfaz VLAN99

### Paso 2: Entre al modo de configuración de interfaz para FastEthernet 0/18 y habilitar la seguridad de puertos.

Entramos en la interfaz Fa 0/18 con el comando **interface**

```
S1(config)#interface fastEthernet 0/18
S1(config-if)#
```

---

Figura 9. Entrar a interface Fa 0/18

Configuramos la seguridad en los puertos con el comando **switchport port-security**.

```
S1(config-if)#switchport port-security
```

Figura 10. Definir seguridad en puerto

### Paso 3: Configure la cantidad máxima de direcciones MAC.

Vamos a establecer la valor máximo 1. Con el comando **switchport port-security maximum 1**.

```
S1(config-if)#switchport port-security maximum 1
```

Figura 11. Definir seguridad máxima en puerto

### Paso 4: Configure el puerto para agregar la dirección MAC a la configuración en ejecución.

Configuramos el puerto agregando la dirección MAC. Hacemos uso del comando **switchport port-security mac-address sticky**.

```
S1(config-if)#switchport port-security mac-address sticky
```

Figura 12. Agregar dirección MAC

Alumno: Miguel Santiago Cervilla

Profesor: Julián García Donaire

Integración de las Tecnologías de la Información en las Organizaciones

Grado Ingeniería Informática

Curso 2018/19

6

**Paso 5: Configure el puerto para que se desactive automáticamente si se infringe la seguridad del puerto.**

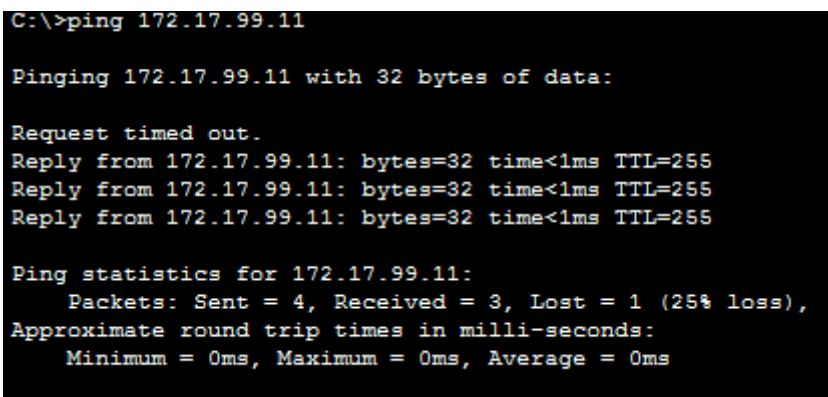
Configuramos el puerto para desactivación automática usando el comando **switchport port-security violation shutdown**

```
S1(config-if)#switchport port-security violation shutdown
```

Figura 13. Comando violation shutdown

**Paso 6: Confirme que S1 ha obtenido la dirección MAC para PC1.**

Para confirmarlo, debemos realizar ping desde **PC1** a **S1**.



```
C:\>ping 172.17.99.11

Pinging 172.17.99.11 with 32 bytes of data:

Request timed out.
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255

Ping statistics for 172.17.99.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura 11. Ping de PC1 a S1

Una vez realizado todo lo anterior, vamos a proceder a realizar otra serie de nuevos pasos para probar la funcionalidad. Los pasos son los siguientes:

**Paso 1: Quite la conexión entre PC1 y S1 y conectar PC2 a S1.**

Desconectamos **PC1** de **S1** y conectamos **PC2** a **S1** en la interfaz **Fa 0/18**.

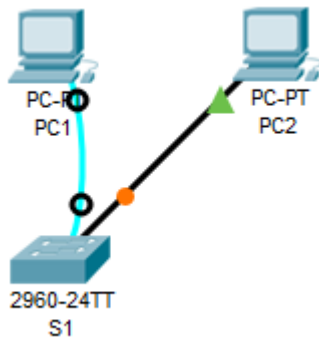


Figura 15. Conectamos PC2 a S1 en Fa 0/18

Probamos a hacer ping de **PC2** a **S1**, esto debería desactivar el puerto al infringirse la seguridad.

```
C:\>ping 172.17.99.11

Pinging 172.17.99.11 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.99.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 16. Ping de PC2 a S1

**Alumno:** Miguel Santiago Cervilla

**Profesor:** Julián García Donaire

Integración de las Tecnologías de la Información en las Organizaciones

Grado Ingeniería Informática

Curso 2018/19

8



Como podemos observar en la **Figura 16**, no hay comunicación entre **PC2** y **S1**. Esto quiere decir que se ha ejecutado correctamente la seguridad del puerto. Para ello nos debería salir en el diagrama de topología en la herramienta, el puerto **Fa 0/18** desactivado.

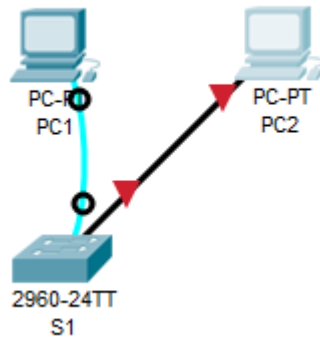


Figura 17. Puerto Fa 0/18 desactivado por seguridad

Como podemos observar en la **Figura 17**, el puerto se ha desactivado debido a la restricción de seguridad.

### Paso 3: Restaure la conexión entre PC1 y S1 y restablecer la seguridad del puerto.

Volvemos a conectar **PC1** a **S1** en el puerto **Fa 0/18**. Procedemos a activar nuevamente el puerto:

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface fa0/18
S1(config-if)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to
administratively down
S1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
S1(config-if)#exit
S1(config)#
```

Figura 18. Activación puerto Fa 0/18

Alumno: Miguel Santiago Cervilla

Profesor: Julián García Donaire

Integración de las Tecnologías de la Información en las Organizaciones

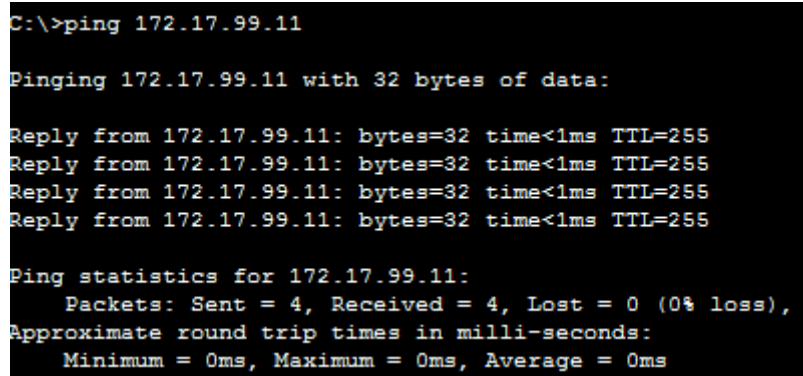
Grado Ingeniería Informática

Curso 2018/19

9

#### **Paso 4: Pruebe la conectividad mediante un ping a S1 desde PC1.**

Probamos nuevamente que existe comunicación entre **PC1** y **S1**. Para ello hacemos uso del comando ping.



```
C:\>ping 172.17.99.11

Pinging 172.17.99.11 with 32 bytes of data:

Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255

Ping statistics for 172.17.99.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura 19. Ping de PC1 a S1

Como podemos observar, el puerto se ha encendido con éxito y si existe comunicación entre **PC1** y **S1**.

Una vez realizado lo anterior, vamos a proteger los puertos sin utilizar. Para ello vamos a seguir los siguientes pasos:

#### **Paso 1: Deshabilite la interfaz Fa0/17 en S1.**

```
S1(config)#interface fa0/17
S1(config-if)#shutdown
```

Figura 20. Deshabilitar interfaz Fa 0/17

#### **Paso 2: Pruebe el puerto mediante la conexión de PC2 a Fa0/17 en S1.**

Para probar que está desactivado el puerto, vamos a observar que al conectar **PC2** al puerto **Fa 0/17**, los enlaces son de color rojo.

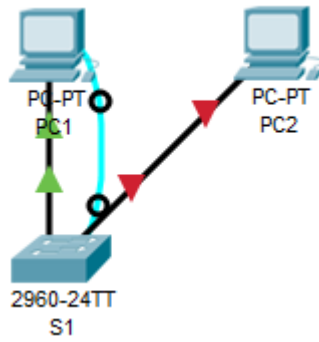


Figura 12. Enlaces de color rojo en Fa 0/17

Una vez completado esto, hemos realizado satisfactoriamente la actividad.

**Alumno:** Miguel Santiago Cervilla

**Profesor:** Julián García Donaire

**Integración de las Tecnologías de la Información en las Organizaciones**

**Grado Ingeniería Informática**

**Curso 2018/19**

**11**

### 3. Conclusiones

En esta práctica hemos aprendido algunas de las funcionalidades que Packet Tracer nos da. Hemos solucionado un problema de creación de una topología. Hemos configurado todos los Host pertenecientes a cada subred, distinguido entre varias subredes, hemos configurado en línea de comandos cada uno de los routers de la actividad y hemos probado que todo funciona correctamente, es decir, usando el comando ping desde cada uno de los host hemos ido probando que la comunicación del mismo era correcta con cada uno de los distintos dispositivos conectados.

Para el cálculo de las direcciones IP, hemos usado las técnicas estudiadas en clase, para el cálculo de las mismas y las máscaras.

Hemos visto la funcionalidad de las distintas conexiones y por qué se da cada una de ellas.

Hemos configurado una VLAN desde el principio..

Hemos realizado una serie de pruebas sobre la comunicación de los dispositivos de la topología.

Hemos configurado la seguridad de los puertos y probado su funcionalidad.

Aparte de todo lo citado anteriormente, esta práctica nos ha enseñado a como diseñar un documento sobre la misma, de una manera clara, concisa, técnica y con una buena presentación.

**Alumno:** Miguel Santiago Cervilla

**Profesor:** Julián García Donaire

**Integración de las Tecnologías de la Información en las Organizaciones**

**Grado Ingeniería Informática**

**Curso 2018/19**

**12**

## 4. Bibliografía

- [1] Las referencias bibliográficas, [consulta 08-02-2017], disponible en [http://ocw.usal.es/eduCommons/ciencias-sociales-1/fuentes-de-informacion/contenidos/LAS\\_REFERENCIAS\\_BIBLIOGRAFICAS.pdf](http://ocw.usal.es/eduCommons/ciencias-sociales-1/fuentes-de-informacion/contenidos/LAS_REFERENCIAS_BIBLIOGRAFICAS.pdf).
- [2] Cisco Networking Academy, [consulta 10-10-2018], disponible en <https://www.netacad.com/es>
- [3] Packet Tracer, [consulta 05-10-2018], disponible en <https://www.netacad.com/es/courses/packet-tracer>
- [4] Servidor de apoyo a la Docencia de Arquitectura de Computadores y Electrónica [consulta 01-10-2018] disponible en <http://sad.ace.ual.es/>
- [5] SlideShare, comandos para cisco [consulta 14-10-2018] disponible en <https://es.slideshare.net/samuelhuertasorjuela/comandos-de-configuracion-de-dispositivos-cisco>
- [6] Blogspot, configuración de un router desde el principio [consulta 01-11-2018] disponible en <http://juanmenr-teleco.blogspot.com/2011/05/configurar-un-router-al-principio.html>
- [7] Cisco , configuración de interfaces de switches [consulta 01-11-2018] disponible en [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2950/software/release/12-1\\_11\\_yj4/configuration/guide/lrescg/swint.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2950/software/release/12-1_11_yj4/configuration/guide/lrescg/swint.pdf)
- [8] Cisco, interface bandwidth [consulta 10-11-2018] disponible en [https://www.cisco.com/c/m/en\\_us/techdoc/dc/reference/cli/nxos/commands/12/bandwidth-interface.html](https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/12/bandwidth-interface.html)
- [9] Cisco, configuración OSPF [consulta 10-11-2018] disponible en [https://www.cisco.com/c/es\\_mx/support/docs/ip/open-shortest-path-first-ospf/118879-configure-ospf-00.html](https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/118879-configure-ospf-00.html)
- [10] Cisco, configuración VLAN [consulta 13-11-2018] disponible en <https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html>

**Alumno:** Miguel Santiago Cervilla

**Profesor:** Julián García Donaire

**Integración de las Tecnologías de la Información en las Organizaciones**

**Grado Ingeniería Informática**

**Curso 2018/19**

**13**