12. APÉNDICES.

Anexo 1 Modos de línea de comando del switch Cisco

Tabla 6: Modos de línea de comando del switch Cisco[27]

Modo	**Método de acceso**	**Prompt**	**Salir o pasar al siguiente modo**
User EXEC	Este es el primer nivel de configuración. Permite cambiar propiedades del terminal, realizar funciones básicas y mostrar información del sistema.	Switch>	Introducir el comando *logout*. Para pasar al modo *privileged* EXEC introducir el comando *enable*.
Privileged EXEC	Desde el modo *User EXEC* introducir el comando *enable*.	Switch#	Para salir al modo *User EXEC* introducir el comando *disable*. Para pasar al modo global de configuración usar el comando configure.
Configuración global	Desde el modo *privileged EXEC* introducir el comando configure	Switch(config)#	Para pasar al modo *privileged* EXEC introducir los comandos *end* o *exit*, o pulsar Ctrl-z.
Configuración de interfaz	Desde el modo de configuración global introducir el comando interface seguido de un identificador de interfaz	Switch(config-if)#	Para pasar al modo *privileged* EXEC introducir el comando *end* o pulsar Ctrl.z. Para pasar al modo de configuración global introducir el comando *exit*.
Config-vlan	Desde el modo de configuración global introducir el comando vlan seguido de un identificador de vlan	Switch(config-vlan)#	Para pasar al modo *privileged* EXEC introducir el comando *end* o pulsar Ctrl-z. Para pasar al modo de configuración global introducir el comando *exit*.
Configuración de VLANs	Desde el modo *privileged* EXEC introducir el comando vlan database	Switch(vlan)#	Para pasar al modo *privileged* EXEC introducir el comando *exit*.
Line configuration	Desde el modo de configuración global especificamos una “línea” usando el comando line	Switch(config-line)#	Para pasar al modo *privileged* EXEC introducir el comando *end* o pulsar Ctrl-z. Para pasar al modo de configuración global introducir el comando *exit*.

Anexo 2 Configuración teléfono IP

En este anexo se va a explicar la configuración necesaria sobre los equipos de comunicación, para la integración y funcionamiento seguro de un teléfono IP y otro dispositivo, normalmente un PC.

Estos tipos de teléfono admiten la conexión de un dispositivo conectado en cascada. Por este motivo la interfaz del switch puede llevar una mezcla de tráfico de datos y voz.

La siguiente figura 81, muestra la configuración realizada para la correcta autenticación del Teléfono IP y del ordenador.

```
!
interface GigabitEthernet0/5
 switchport mode access
 switchport nonegotiate
 authentication event fail action authorize vlan 69
 authentication event no-response action authorize vlan 69
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast edge
!
```

Figura 81: Configuración interfaz teléfono y pc

Este puerto del switch está configurado de tal forma, que los dispositivos de acceso tienen que autenticarse a través del protocolo 802.1X. En este caso si los datos de usuario son introducidos incorrectamente o el método de autenticación no responde, el switch directamente coloca a este usuario que está intentando acceder a la red, a una VLAN restringida. En este caso la VLAN 69, denominada puertos_inactivos, como se muestra en la figura 82.

```
COM3 - PuTTY
face Gi0/5 AuditSessionID C0A840020000008A28394E9A
Switch-LabInycom#
Dec 30 09:11:20.091: %DOT1X-5-RESULT_OVERRIDE: Authentication result overridden for client (80
5e.c0e1.67c8) on Interface Gi0/5 AuditSessionID C0A840020000008A28394E9A
Switch-LabInycom#sh vla
Switch-LabInycom#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                                Gi0/6, Gi0/8, Gi0/10, Gi0/11
                                                Gi0/12
65   Administradores                  active
66   Invitados                        active
67   Marketing                        active
68   Recursos_humanos                 active
69   puertos_inactivos                active    Gi0/5
```

Figura 82: Fallo de autenticación VLAN 69

Una vez confirmada la autenticación del teléfono IP, este es colocado directamente en la VLAN de voz correspondiente. Pero otro factor a tener en cuenta es, que por defecto la configuración del puerto solo permite una dirección MAC. Por lo tanto cuando intentemos conectar un ordenador en cascada con el teléfono, el puerto se deshabilitará y no tendremos acceso. Esto se muestra en la figura 83, donde el estado del puerto GigabitEthernet0/5 pasa a *err-disabled*.

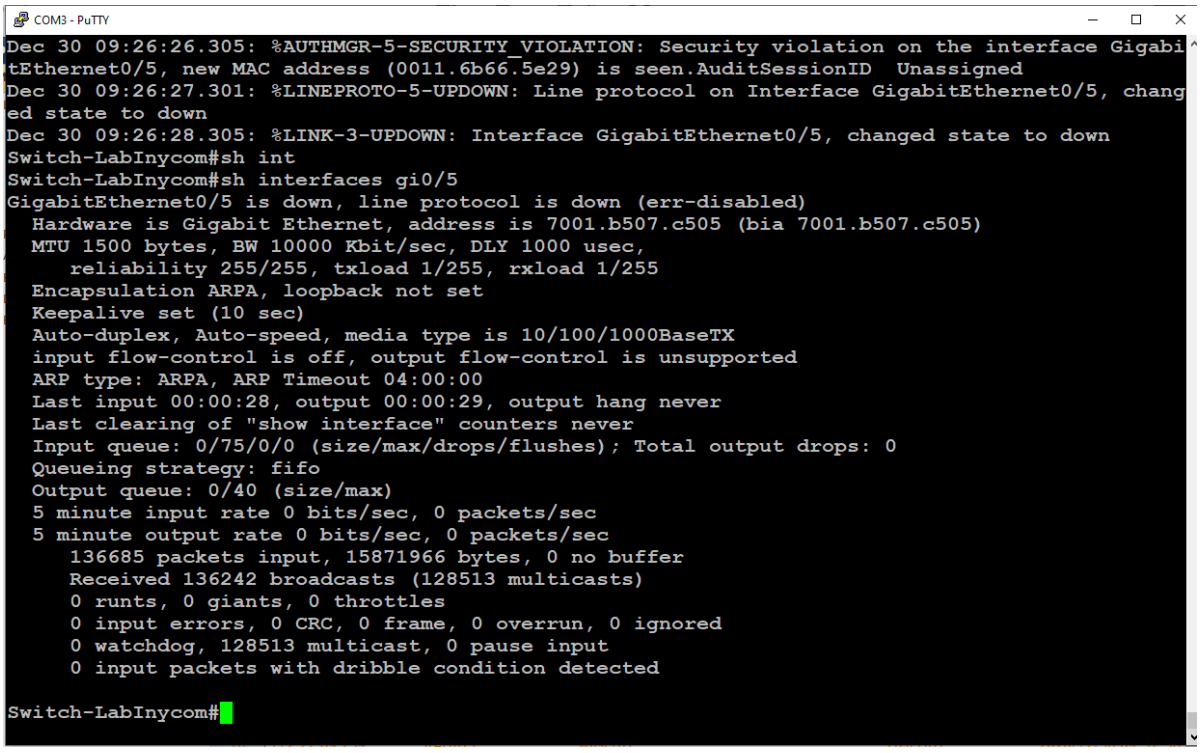

Figura 83: Múltiples dispositivos sin autorización

Para solucionar esto es imprescindible el siguiente comando observado anteriormente en la figura 80.

authentication host-mode multi-auth

Esta instrucción permite autenticar varios hosts en un solo puerto, pudiendo estos utilizar diferentes métodos. Cada host se autentica individualmente antes de que pueda acceder a los recursos de la red y permite un cliente en la VLAN de voz y varios clientes en la VLAN de datos.

En la imagen 84 se observa como una vez finalizada la autenticación de los dos dispositivos, cada uno accede a una VLAN distinta, a la VLAN 102 el ordenador y a la Voice_VLAN el teléfono IP.

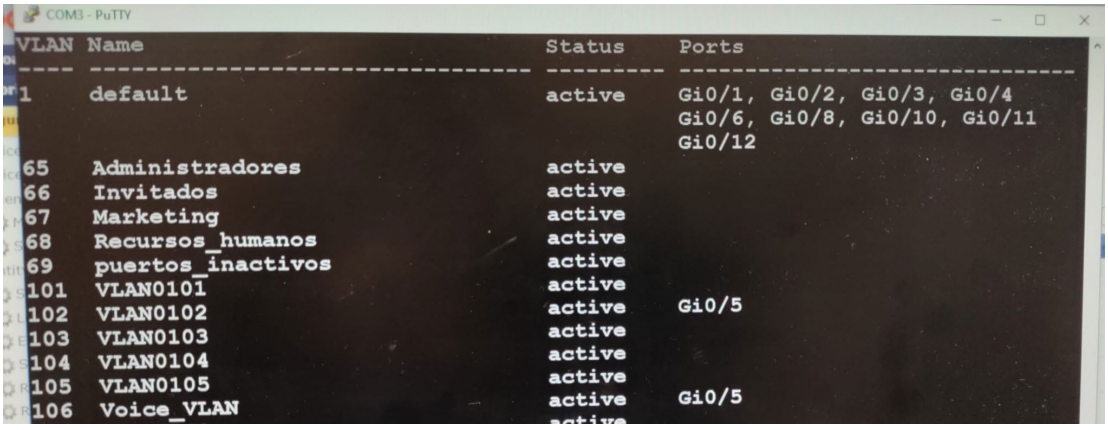

Figura 84: Interfaces con sus respectivas VLANs

Anexo 3 Distintas configuraciones de seguridad 802.1X

En este apartado vamos a explicar las posibles configuraciones que podemos utilizar para la autenticación IEEE 802.1X.

Como hemos comentado durante el trabajo, esta medida de seguridad se configura en puertos donde se vayan a conectar usuarios finales y queremos evitar que dispositivos no autorizados obtengan acceso a la red.

Configuración estándar 802.1X

```
switchport mode access
switchport nonegotiate
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
mab
dot1x pae authenticator
spanning-tree portfast
```

Configuración fallo autenticación 802.1X

```
switchport mode access
switchport nonegotiate
authentication event fail action authorize vlan 10
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
mab
dot1x pae authenticator
spanning-tree portfast
```

Configuración sin suplicante 802.1X

```
switchport mode access
switchport nonegotiate
authentication event no-response action authorize vlan 1
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
mab
dot1x pae authenticator
spanning-tree portfas
```

Anexo 4 Pasos a seguir en configuración de switch

1. Consejos previos a la configuración

- Configurar nombre de equipo.
- Definir política de contraseñas.
- Creación de cuentas con privilegios de usuario y administrador.
- Configurar tiempo de inactividad.
- Añadir mensaje de banner.

2. Servicios de red para la gestión del switch

- Deshabilitar HTTP/HTTPS.
- Deshabilitar TELNET.
- Configurar SNMPv3 si es necesario.

3. Seguridad basada en puertos

- Deshabilitar puertos inactivos.
- Limitar mensajes que llegan a los puertos, *Storm Control*.
- Definición de MAC seguras.
- Limitar número de MACs.
- Creación de ACLs.

4. VLANs

- VLAN diferente para enlaces inactivos.
- Cambiar todos los puertos que no sean de gestión a una VLAN diferente a la nativa.

5. STP

- Configurar puertos de acceso como *Port Fast*.
- Habilitar *BPDU Guard*.
- Uso de *Root Guard*.

6. Registros: Logs

- Configurar registros y depuración de mensajes.
- Configurar servidor NTP.

7. Protocolo AAA

- Configuración de un servicio de acceso a los servidores de seguridad.