Configuración de Swicht CISCO-300-x (series) con 'Vlan's' diferenciadas y configuración a traves de ssh para configurar Trunk's → Meraki VPN de acceso remoto Multiplataforma.

* Previo a cualquier tipo de configuración, es importante planificar como será el acceso a los puertos de las diferentes VLANs.

* Debemos considerar como buena práctica, dedicar el puerto número 1, como administrativo. Si, será nuestro acceso al switch y lo perderemos para otras cuestiones, porque será partícipe de la VLAN nativa número 1 (insustituible y nativa por definición, y no etiquetable).

* Como buena praxis es aconsejable ahora dispersar, y en aras de la seguridad una evidencia tan clara. Es importante considerar otro ID de Vlan como nativa. (Al respecto es importante conocer el número máximo y su prelación). Habitualmente suele utilizarse el número 99 como '**VLAN nativa adquirida**'.

* Ahora como hipótesis de trabajo utilizaremos estos ID de Vlan:

→ **10** → Administrativo. → 192.168.10.0/24.
→ **50** → Técnico. → 192.168.50.0/24.
→ **1** → Troncal Nativo.
→ **99** → Troncal adquirido de forma Nativa (No Etiquetable).

* Es hora de analizar nuestro Switch, y en este caso de la serie SG-300 y 20 puertos, de los cuales 2 serán de Fibra óptica/mixtos (Ojo con los transceptores. No son todos iguales !!!. Por eso me encanta **CISCO**).

Planteamiento del caso:

→ **Puerto 1**	→ **VLAN 1**	**=> Extríctamente Administrativo.**
→ **Puertos 2 al 15**	→ **VLAN 10**	**=> OFICINAS CENTRALES.**
→ **Puertos 19 al 20**	→ **VLAN 50**	**=> OFICINA TÉCNICA.**
→ **Puertos 8,16,17,18**	→ **VLAN 99**	**=> Troncal Adquirido por Seguridad.**

* Es importante observar los puertos asignados en la VLAN 99.

* El puerto 17 será el Link para un puerto LAN de nuestro Firewall Meraki. (La teoria clásica recomendaba hacer un Link por los diversos troncales de las diferentes VLANś).

* Es importante tener en cuenta que la reserva de puertos **8-16-17-18** es para un futuro y previsible **LACP** o **LAG** y para poder aumentar el ancho de banda o agregar/enlazar Switches.
* Pero lo mas importante es: Que la disposición del Switch o Switches es en capa 2 según el modelo OSI de 7 capas → APSTREF (Aplicación-Presentación-Sesión-Transporte-Red-Enlace-Física). ==> Nunca en capa 3 o Layer 3.
Esto es, porque un Switch Gestionable puede hacer muchas cosas, en realidad casi todo. Pero su mejor cometido No es -Enrutar- aunque lo haría en capa 3 y poco efectivamente.

* La función de enrutamiento la realiza de forma fantástica un Router o un Firewall, al mismo tiempo que realiza todos los filtrados necesarios y en diferentes capas: Capa 3, 2 o Capa 7, e incluso como IDS (intrusiones detectadas, listas blancas, etc, …). Y seguro que 5 veces mas rápido.

* Por último es importante que el router de acceso de nuestra compañía favorita -NO HAGA NADA-. Es decir que se comporte de forma transparente o en modo brigde. Pero esto es otra cuestión, sencilla pero **Imprescindible**.

==> Con el mapa de nuestro Switch y habilitado ssh por ejemplo, la configuración es inmediata para el plan expuesto:

```
ip ssh server
!
interface vlan 1
 ip address 192.168.10.10 255.255.255.0
 no ip address dhcp
!
interface vlan 10
 name "OFICINA CENTRAL"
!
interface vlan 50
 name "FIBRA OPTICA"
!
interface vlan 99
 name TRONCAL
!
interface gigabitethernet2
 switchport mode access
```

```
 switchport access vlan 10
!
interface gigabitethernet3
 switchport mode access
 switchport access vlan 10
!
interface gigabitethernet4
 switchport mode access
 switchport access vlan 10
!
interface gigabitethernet5
 switchport mode access
 switchport access vlan 10
!
interface gigabitethernet6
 switchport mode access
 switchport access vlan 10
!
interface gigabitethernet7
 switchport mode access
 switchport access vlan 10
!
interface gigabitethernet8
 switchport trunk allowed vlan add 10,50
 switchport trunk native vlan 99
!
interface gigabitethernet9
 switchport mode access
 switchport access vlan 10
!
interface gigabitethernet10
 switchport mode access
 switchport access vlan 10
!
interface gigabitethernet11
 switchport mode access
 switchport access vlan 10
!
interface gigabitethernet12
 switchport mode access
 switchport access vlan 10
```

```
!
interface gigabitethernet13
 switchport mode access
 switchport access vlan 10
!
interface gigabitethernet14
 switchport mode access
 switchport access vlan 10
!
interface gigabitethernet15
 switchport mode access
 switchport access vlan 10
!
interface gigabitethernet16
 switchport trunk allowed vlan add 10,50
 switchport trunk native vlan 99
!
interface gigabitethernet17
 switchport trunk allowed vlan add 10,50
 switchport trunk native vlan 99
!
interface gigabitethernet18
 switchport trunk native vlan 99
!
interface gigabitethernet19
 switchport mode access
 switchport access vlan 50
!
interface gigabitethernet20
 switchport mode access
 switchport access vlan 50
!
exit
```

* Otro día vemos como hacer un brigde en un router apócrifo y las reglas ACL de un cortafuegos hardware.