

**Ejercicio 22. VLANs y listas de control de acceso (ACLs)**

#### En la realización de estos ejercicios debes considerar como independiente cada una de las ACLs. Para probar las ACLs en PT se te recomienda desactivar las ACLs previas a cada inciso.

#### Utiliza la información de la siguiente gráfica y diseña cada una de las listas de control de acceso solicitadas.

Diagrama

Descripción generada automáticamente

Mejores prácticas para el diseño de ACLs

1. Identificar la fuente/origen (tráfico fuente)
2. Identificar el tráfico no permitido. trayecto de la fuente al destino Trazar el flujo de tráfico
3. Identificar el tráfico permitido.
4. Identificar el router donde se instalará la lista de control de acceso.
5. Identificar la interfaz donde se va a asociar la lista de control de acceso.
6. Determinar la interface donde se va a insertar la lista de acceso.

**REGLA, LA LISTA DE ACESO ESTÁNDAR SE DEBEN INSTALAR LO MAS CERCA DEL DESTINO.**

1. Diseña una lista de control de acceso estándar para **impedir** que las computadoras de la VLAN de **Entretenimiento** tengan acceso a la VLAN de **HomeOffice**.

**access-list 10 deny 192.168.10.128 0.0.0.63**

**access-list 10 permit any**

**int g0/1.10**

**ip access-group 10 out**

1. Diseña una lista de control de acceso estándar para que el **SmartPhone** no pueda acceder a la VLAN de **HomeOffice**

**access-list 20 deny host 192.168.10.142**

**access-list 20 permit any**

**int g0/1.10**

**ip access-group 20 out**

1. Diseña una lista de control de **acceso extendida** para **impedir** que las computadoras de la VLAN de **Entretenimiento** tengan acceso a la VLAN de **HomeOffice**.

**access-list 110 deny ip 192.168.10.128 0.0.0.63 192.168.10.0 0.0.0.127**

**access-list 110 permit ip any any**

**int g0/1.20**

**ip access-group 110 in**