Capas de Acceso en Redes Locales, Protocolos y Fundamentos

Objetivos:

- Comprender y diferenciar distintos tipos de redes, y métodos de acceso al medio.
- Conocer los estándares IEEE 802.3 y 802.11, sus evoluciones y diferencias clave entre versiones.
- Practicar con dispositivos de red locales: NIC, Switch y Router.
- Configurar VLANs, NAT, ACLs.

Requisitos:

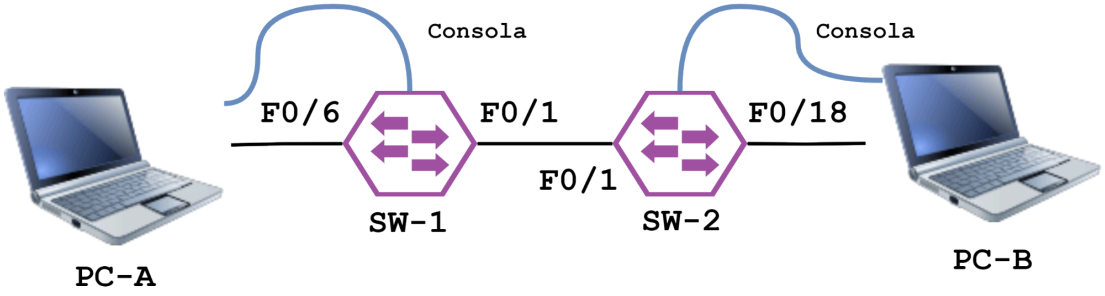
- Acceso a una computadora con Wi-Fi y acceso a Internet.
- Bibliografía de la materia.
- Packet Tracer.

Consignas:

1) Alcance de Redes y Virtualización

   a) Investigar cómo se clasifican las redes según su alcance. Mencionar brevemente las características principales de cada una y colocar en cada cuadro de la Figura el acrónimo de red que corresponda.
   b) ¿Qué es una VLAN? ¿Cómo se clasifican?
   c) Investigar y resumir el protocolo IEEE 802.1Q. ¿Cómo se relaciona con las VLAN?
   d) En el contexto de los dos ítems anteriores ¿Qué es el Tagging?

2) Implementaremos la siguiente topología en Packet-Tracer:



Con la siguiente Tabla de ruteo:

Device	Interface	IP Address	Subnet Mask	Default Gateway
SW-1	VLAN 1	192.168.1.11	255.255.255.0	N/A
SW-2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.4	255.255.255.0	192.168.10.1

a) Desde cada computadora, ingresar a la terminal y configurar los switch. Nombrar a los mismos sw1 y sw2 respectivamente. Ayuda: investigar los comandos necesarios online si no te acordás, por ejemplo, para cambiar el nombre del switch:

```
switch>
switch>en
switch#conf t
switch(config)#hostname nombre
```

b) Asignar contraseñas privilegiadas, de consola y vty. Ayuda:

```
enable secret contrasena_exec
line console 0
password contrasena_consola
login
exit
line vty 0 15
password contrasena_vty
login
exit
```

c) Encriptar las contraseñas (Ayuda: utilizar `service password-encryption`)
d) Configurar las redes VLAN para ambos switch según la tabla de direcciones provista. Ayuda:

```
interface vlan 1
ip address <IP_address> <subnet_mask>
no shutdown
exit
```

e) Desconectar todas las interfaces que no estén siendo utilizadas (Ayuda: podés ver las interfaces utilizando `show ip interface brief`)
f) Guardar la configuración (`write memory`)
g) Testear comunicación usando pings entre las computadoras.
h) Crear VLANs en ambos switches. Ayuda:

```
sw1(config)# vlan 10
sw1(config-vlan)# name Laboratorio
sw1(config-vlan)# vlan 20
sw1(config-vlan)# name Bar
sw1(config-vlan)# vlan 99
sw1(config-vlan)# name Management
sw1(config-vlan)# end
```

i) Utilizar `show vlan brief` para visualizar la lista de VLANs en alguno de los switch. ¿Cuál es la VLAN utilizada por defecto?. Colocar el output en el informe.
j) Asignar la PC-A a la VLAN Laboratorio. Ayuda:

```
sw1(config)# interface f0/6
sw1(config-if)# switchport mode access
sw1(config-if)# switchport access vlan 10
```

k) Desde la VLAN 1, remover la ip de Management y configurarla para funcionar en la VLAN 99 (que configuramos como Management). Ayuda:

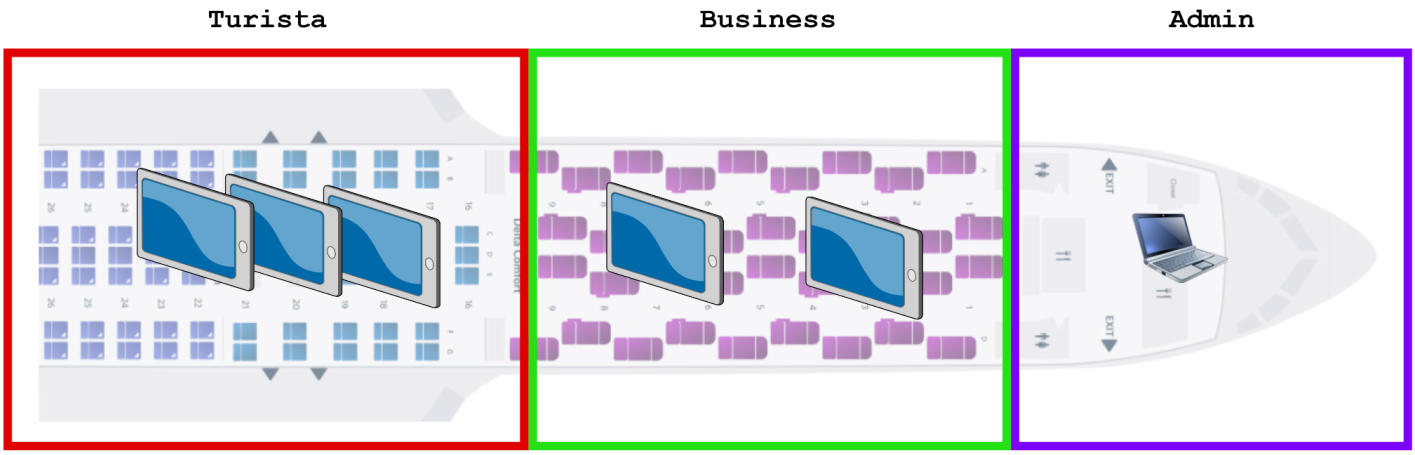
```
sw1(config)# interface vlan 1
sw1(config-if)# no ip address
sw1(config-if)# interface vlan 99
sw1(config-if)# ip address IP MASCARA
sw1(config-if)# end
```

l) Verificar el estado de la VLAN utilizando `show vlan brief` y el estado de las interfaces utilizando `show ip interface brief`. Colocar los output en el informe e interpretar.
m) Asignar la PC-B a la VLAN Laboratorio en el sw2. Repetir el inciso k) pero para el sw2.
n) Verificar la conectividad entre PC-A y PC-B utilizando pings. Verificar conectividad entre sw1 y sw2 utilizando pings. Interpretar los resultados.

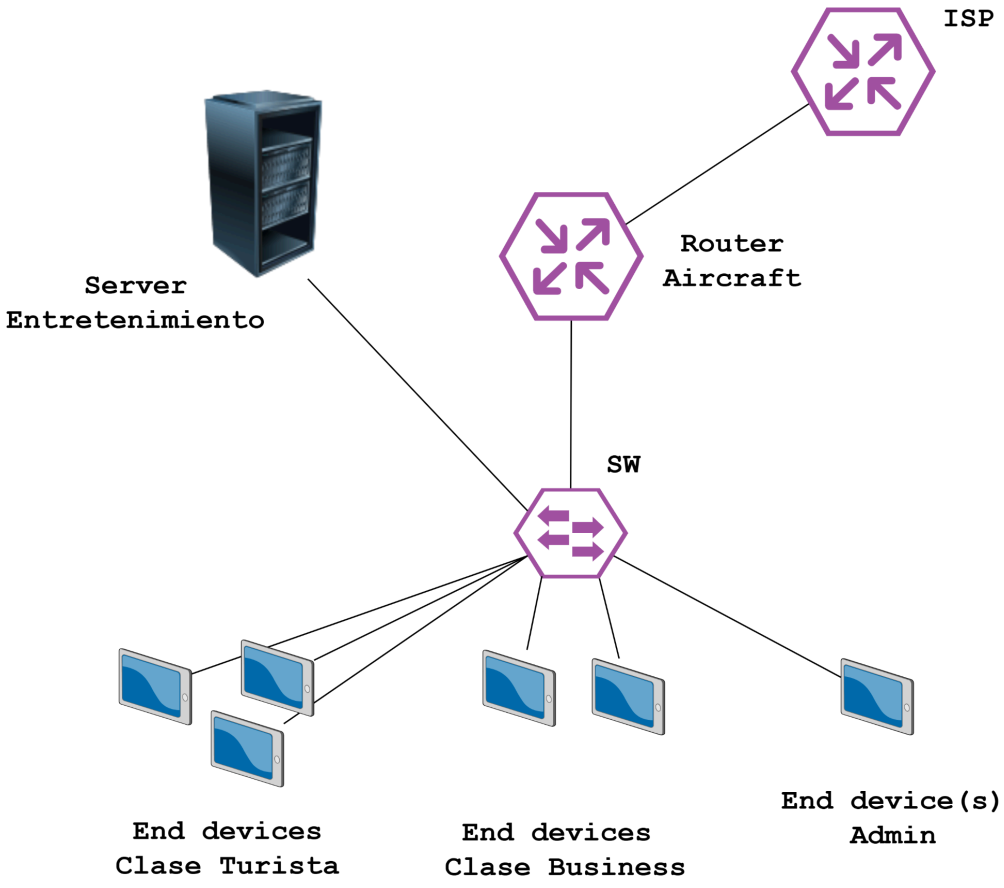
Si necesitás más ayuda podés consultar este ejercicio de Cisco. Cuidado al aplicar los comandos!, siempre hay que estar seguros de estar ubicado en el directorio/programa que corresponda. Cuidado al copiar componentes!, se van a copiar las configuraciones (como passwords, usuarios, vlans, etc.).

3) Utilizando lo que aprendimos sobre VLAN, e investigando la configuración de NAT y ACLs, simularemos el despliegue de una red LAN a bordo de una aeronave. La idea es la siguiente, tendremos tres segmentos:

i) Clase Turista: acceso solo a un sistema de entretenimiento (server local)
ii) Clase Business: acceso a sistema de entretenimiento e internet.
iii) Administración: acceso total.



Podés usar una topología de red como la siguiente:



Y la siguiente tabla de direccionamiento:

VLAN	Nombre	Red IP	Gateway	Acceso
10	Turista	10.10.10.0/24	10.10.10.1	Solo servidor
20	Business	10.10.20.0/24	10.10.20.1	Servidor + Internet
99	Administración	10.10.99.0/24	10.10.99.1	Acceso total
—	Enlace ISP	200.0.0.0/30	200.0.0.1–.2	—

Pero como ya saben: pueden modificar lo que necesiten en tanto el espíritu de la actividad se mantenga.

Luego de configurar la red realizarán las siguientes pruebas:

Prueba	Desde	Hacia	Resultado esperado
Ping al servidor de entretenimiento	PC Turista	10.10.99.10	✅ Responde
Acceso HTTP a servidor local	PC Turista	http://10.10.99.10	✅ Carga la página
Ping a Internet	PC Turista	—	❌ Bloqueado
Acceso HTTP a servidor local	PC Business	http://10.10.99.10	✅ Carga
Ping a Internet (ej: 8.8.8.8)	PC Business	—	✅ Funciona
Ping entre Admin y todos	Admin PC	—	✅ Todos

Por supuesto pueden simular “internet” con cualquier cosa que responda del lado del ISP.

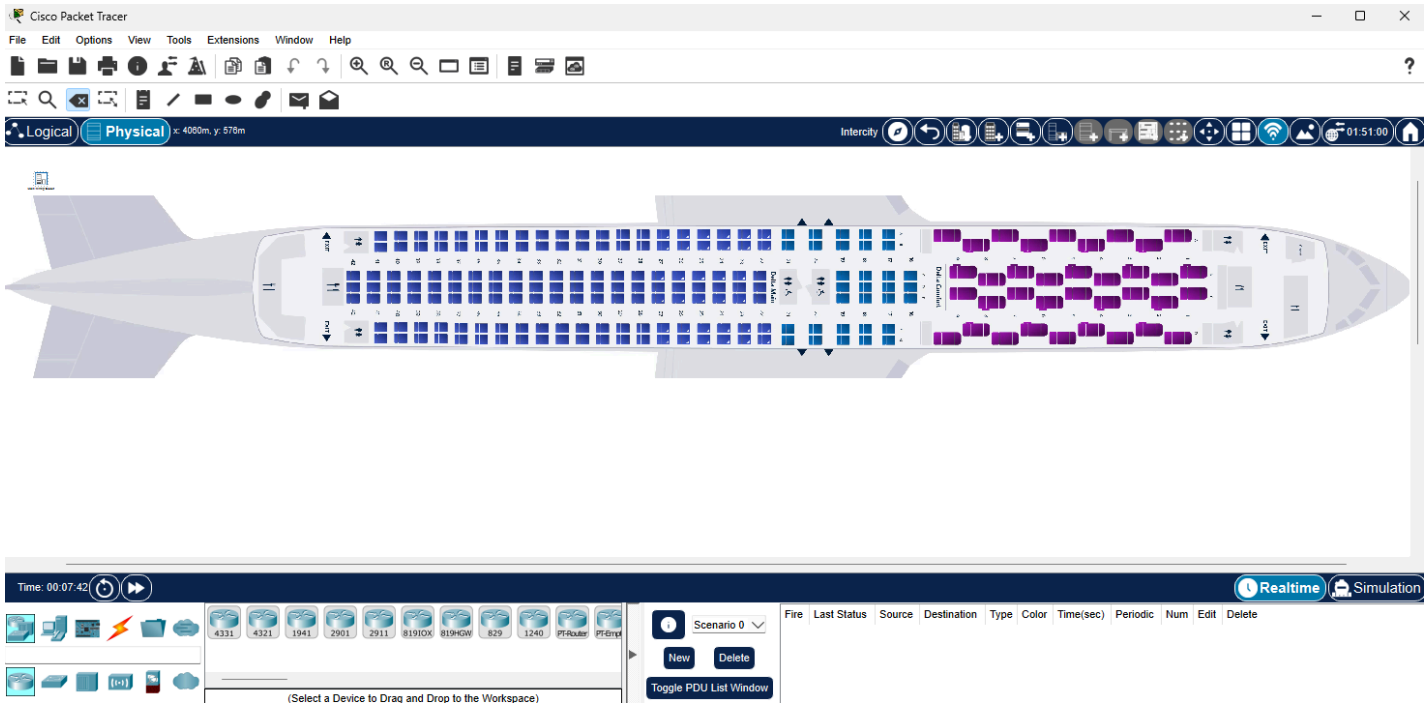
Detallar en el informe el diagrama de red (hecho en PT), capturas de pantalla, y conclusiones.

*Ayudas (**NO es necesario que utilicen al pié de la letra nada de esto**):*

Para simular el servidor de entretenimiento pueden utilizar el mismo servicio HTTP que ya viene por defecto con los servidores de Packet Tracer. Pueden modificar o agregar un documento .html a su gusto a los efectos de simular el servicio:

```
<html>
  <h1>🎬 AirConnect Entertainment</h1>
  <p>Bienvenido a bordo. Disfrute nuestras películas y música.</p>
</html>
```

Pueden utilizar, si así lo quisieran, la imágen que deseen como background en Packet Tracer:



Configuración del router del avión:

```
enable
configure terminal

! Subinterfaces para VLANs
interface FastEthernet0/0
 no shutdown
```

```
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.10.10.1 255.255.255.0
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.10.20.1 255.255.255.0
!
interface FastEthernet0/0.99
 encapsulation dot1Q 99
 ip address 10.10.99.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 200.0.0.1 255.255.255.252
 no shutdown

! DHCP para cada clase
ip dhcp excluded-address 10.10.10.1 10.10.10.10
ip dhcp excluded-address 10.10.20.1 10.10.20.10
ip dhcp excluded-address 10.10.99.1 10.10.99.10

ip dhcp pool Turista
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1
 dns-server 10.10.100.10

ip dhcp pool Business
 network 10.10.20.0 255.255.255.0
 default-router 10.10.20.1
 dns-server 8.8.8.8

ip dhcp pool Admin
 network 10.10.99.0 255.255.255.0
 default-router 10.10.99.1
 dns-server 8.8.8.8

! NAT solo para VLAN20 (Business)
access-list 20 permit 10.10.20.0 0.0.0.255
ip nat inside source list 20 interface FastEthernet0/1 overload
```

```
! Marcar interfaces NAT
interface FastEthernet0/0.10
 ip nat inside
!
interface FastEthernet0/0.20
 ip nat inside
!
interface FastEthernet0/0.99
 ip nat inside
!
interface FastEthernet0/1
 ip nat outside

! Bloquear Internet a VLAN10 (Turista)
access-list 100 deny ip 10.10.10.0 0.0.0.255 any
access-list 100 permit ip any any
interface FastEthernet0/0.10
 ip access-group 100 out

! Ruta por defecto hacia ISP
ip route 0.0.0.0 0.0.0.0 200.0.0.2
```

Configuración del Switch:

```
enable
configure terminal

vlan 10
 name Turista
vlan 20
 name Business
vlan 99
 name Admin

! Puerto hacia router como trunk
interface FastEthernet0/1
 switchport mode trunk

! Asignar puertos a cada clase
```

```
interface range FastEthernet0/2 - 3
 switchport mode access
 switchport access vlan 10

interface range FastEthernet0/4 - 5
 switchport mode access
 switchport access vlan 20

interface FastEthernet0/6
 switchport mode access
 switchport access vlan 99

interface FastEthernet0/7
 switchport mode access
 switchport access vlan 99  ! para el servidor
```