SESIÓN DE LABORATORIO 3
Configuración de VLAN

Objetivos

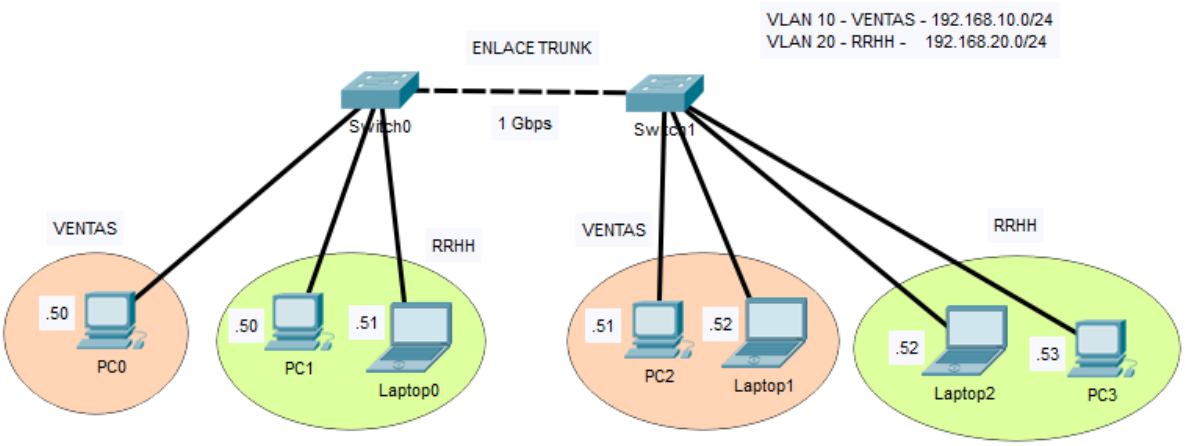
- Entender la utilidad de las VLAN.
- Configurar una red con varias VLAN.
- Comprobar la conexión entre hosts dentro de la misma VLAN.
- Distinguir entre enlaces en modo acceso y en modo troncal.

Desarrollo

Una VLAN se puede definir como una tecnología de Capa 2 que permite la segmentación de la red de manera lógica, logrando que dispositivos conectados al mismo switch o a diferentes switches puedan pertenecer a distintos segmentos de red sin necesidad de un router. En principio, los dispositivos situados en diferentes VLAN no pueden comunicarse entre sí. Cada VLAN se convierte así en un dominio de broadcast distinto, lo que propicia un mejor aprovechamiento del ancho de banda.

En esta sesión diseñaremos la red de área local de una pequeña o mediana empresa implementada con switches Cisco Catalyst 2960. Daremos de alta dos VLAN, una para los dispositivos del Departamento de Ventas (VENTAS) y otra para el Departamento de Recursos Humanos (RRHH). Como veremos, la asignación de VLAN se llevará a cabo en las interfaces de los switches.

Se hará uso de dos subredes IP distintas: 192.168.10.0/24 para VENTAS y 192.168.20.0/24 para RRHH. Dentro de cada subred las direcciones de host empezarán a partir de la dirección .50. La topología a implementar se indica en la siguiente figura, en la cual se distinguen dos switches conectados mediante un enlace (cable cruzado) de tipo troncal (trunk) de 1 Gbps de ancho de banda.



Beneficios de las VLAN

La segmentación de una red mediante el uso de VLAN, una tecnología de Capa 2, aporta los siguientes beneficios:

- Seguridad: a no ser que se resuelva de manera explícita, los miembros de VLAN distintas no pueden comunicarse entre sí.
- Coste: se puede segmentar la red sin necesidad de utilizar routers, dispositivos estos más caros que los switches.
- Rendimiento: el uso de VLAN permite reducir el volumen de tráfico en la red, por lo que las comunicaciones se pueden llevar a cabo más rápidamente. Al mismo tiempo, las tormentas de broadcast afectan solamente a los dispositivos de una VLAN sin afectar al resto.
- Segregación lógica de la red: gracias a las VLAN, dispositivos que no están ubicados físicamente en el mismo lugar ni conectados al mismo switch pueden formar parte de la misma subred.

Creación de las VLAN

En primer lugar comenzaremos creando las VLAN en los switches y asignando un nombre que actuará como descripción. Para ello se usan los comandos siguientes desde el modo de configuración global de cada switch:

```
Switch0#configure terminal
Switch0(config)#vlan 10
Switch0(config-vlan)#name VENTAS
Switch0(config-vlan)#exit
Switch0(config)#vlan 20
Switch0(config-vlan)#name RRHH
Switch0(config-vlan)#exit
```

Asignación de una VLAN a cada interfaz

Una vez dadas de alta las VLAN hay que establecer, para cada interfaz, la VLAN a la que pertenece. A continuación se indica cómo llevar a cabo la asignación a dos de los hosts del

Departamento de Recursos Humanos (VLAN 20) que están conectados en las interfaces Fa0/2 y Fa0/3:

```
Switch0#configure terminal
Switch0(config)#interface range fastEthernet 0/2-3
Switch0(config-if-range)#switchport mode access
Switch0(config-if-range)#switchport access vlan 20
Switch0(config-if-range)#exit
Switch0(config)#
```

Verificación de la configuración de VLAN

Una vez creadas las VLAN y asignada cada interfaz a una de las VLAN, conviene inspeccionar que este proceso de configuración se ha llevado a cabo de forma correcta. Para ello se puede usar el siguiente comando:

```
Switch0#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/2
10   VENTAS                           active    Fa0/1
20   RRHH                             active    Fa0/2, Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

De acuerdo con la información mostrada, podemos comprobar que las interfaces Fa0/2 y Fa0/3 pertenecen a la VLAN 20, cuyo identificador es RRHH, y también que la interfaz Fa0/1 pertenece a la VLAN 10, cuyo identificador es VENTAS. El resto de interfaces pertenecen a la VLAN 1, que es la VLAN nativa por defecto en los switches Cisco. Las VLAN 1002 hasta la 1005 son reservadas, vienen incluidas en la configuración por defecto y no pueden ser eliminadas.

Verificación de la conectividad dentro de cada VLAN

Debería comprobarse ahora que los hosts pertenecientes a una VLAN tienen conectividad entre sí. Para ello hay que cerciorarse de que se ha configurado adecuadamente la dirección IP y la máscara en cada host.

Veamos que hay conectividad entre los dispositivos PC1 y Laptop0 de la VLAN 20 (RRHH) conectados a uno de los switches. Hacemos un ping desde PC1 al Laptop0, y podemos deducir que los cuatro paquetes ICMP (echo request) han llegado al destino y los cuatro paquetes ICMP (echo reply) se han transmitido desde el destino hasta el origen.

```
C:\>ping 192.168.20.51

Pinging 192.168.20.51 with 32 bytes of data:

Reply from 192.168.20.51: bytes=32 time=1ms TTL=128
Reply from 192.168.20.51: bytes=32 time<1ms TTL=128
Reply from 192.168.20.51: bytes=32 time<1ms TTL=128
Reply from 192.168.20.51: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.20.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Creación del enlace trunk

En redes corporativas es usual el uso de varios switches, por lo que es necesario permitir que los hosts de la misma VLAN tengan conectividad entre sí, independientemente del switch al que estén conectados. En principio, la solución pasaría por establecer tantos enlaces entre los switches como VLAN existentes, donde cada uno de ellos se encargaría de transportar el tráfico de aquella VLAN para la que ha sido configurado. Sin embargo, este enfoque es poco práctico y escalable.

La solución más recomendable es la creación de un único enlace, llamado trunk o troncal, que transporte el tráfico de todas las VLAN. Para ello hace falta añadir un campo adicional a las tramas de capa 2, denominado VLAN ID. El protocolo IEEE 802.1Q responde a esta necesidad, agregando una etiqueta de 4 bytes después de la dirección origen. Dentro de esta etiqueta hay 12 bits que indican la VLAN, por lo que en principio podría haber hasta un máximo de $2^{12} = 4096$ VLAN distintas.

A continuación mostramos cómo crear el enlace trunk entre los dos switches de la red. En particular, indicamos el proceso en uno de los switches, proceso que habría que llevar a cabo también en el otro switch.

```
Switch0#configure terminal
Switch0(config)#interface gigabitEthernet 0/1
Switch0(config-if)#switchport mode trunk
Switch0(config-if)#switchport trunk allowed vlan 10,20
Switch0(config-if)#exit
Switch0(config)#
```

Si se omitiera el segundo comando `switchport` el enlace permitiría el paso del tráfico de todas las VLAN existentes. Sin embargo, por motivos de seguridad, es conveniente configurarlo para permitir el paso únicamente de las VLAN estrictamente necesarias.

Ahora si se ejecutase el comando `show vlan brief` veríamos que la interfaz Gi0/1 ya no aparece asociada a ninguna VLAN porque ha sido configurada como troncal:

```
Switch0#show vlan brief

VLAN Name                              Status    Ports
```

```
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/2
10   VENTAS                           active    Fa0/1
20   RRHH                             active    Fa0/2, Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Una de las características de los enlaces troncales es el uso de una **VLAN nativa**, necesaria para etiquetar el tráfico de las interfaces que no han sido configuradas dentro de ninguna VLAN, así como del tráfico "especial" que genera el propio switch (logs, SNMP o conexiones vía telnet). Por defecto, la VLAN nativa es la 1; si se cambiase por alguna razón, debería hacerse el cambio en los dos switches que conforman el enlace. La configuración del enlace trunk es necesaria en ambos extremos con el fin de evitar problemas o el bloqueo de tráfico.

Verificación del enlace trunk

Para verificar el estado del enlace troncal se usa el siguiente comando:

```
Switch0#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      10,20

Port        Vlans allowed and active in management domain
Gig0/1      10,20

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      10,20
```

Otra manera de comprobarlo es mediante el comando `show interfaces Gi0/1 switchport`, que da información detallada de la configuración de esta interfaz concreta:

```
Switch0#show interfaces Gi0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
```

```
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 10,20
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Verificación de la conectividad dentro de cada VLAN

Finalmente, una vez configurado el enlace troncal entre los dos switches es necesario comprobar la comunicación entre hosts de la misma VLAN ubicados en switches distintos, para asegurarnos de que el enlace trunk lleva tráfico de las dos VLAN.

En este caso haremos un ping desde el PC0 al Laptop1 del Departamento de VENTAS para comprobar la conectividad de la red:

```
C:\>ping 192.168.10.52

Pinging 192.168.10.52 with 32 bytes of data:

Reply from 192.168.10.52: bytes=32 time<1ms TTL=128
Reply from 192.168.10.52: bytes=32 time<1ms TTL=128
Reply from 192.168.10.52: bytes=32 time<1ms TTL=128
Reply from 192.168.10.52: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.52:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

EtherChannel entre los switches

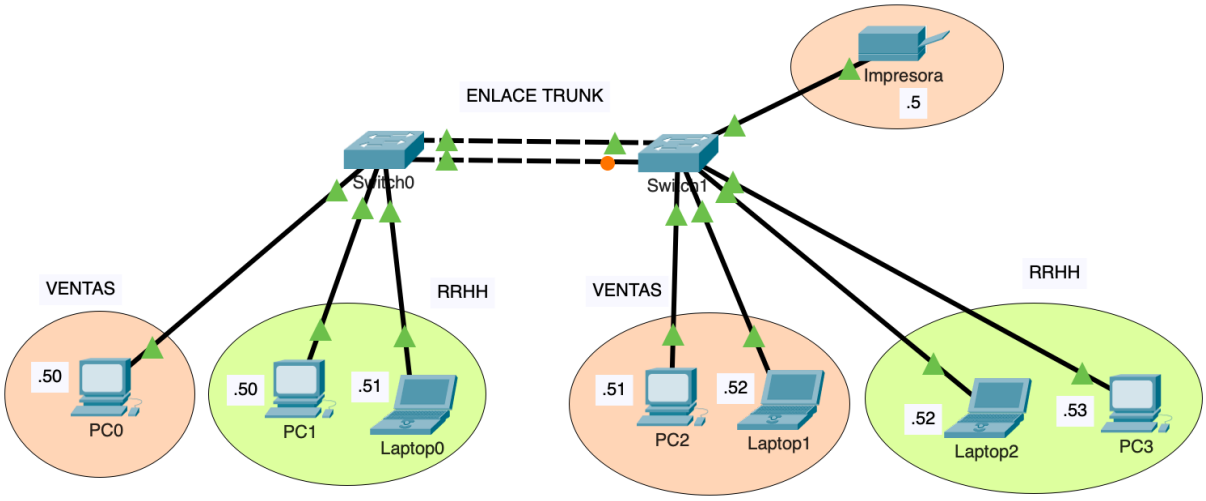
En este apartado vamos a incrementar el ancho de banda de la conexión entre los dos switches haciendo uso de la tecnología Etherchannel. Utilizaremos las dos interfaces GigabitEthernet de ambos conmutadores para conseguir un enlace con un ancho de banda total de 2 x 1 Gbps = 2 Gbps.

Para ello, lo primero que haremos es borrar la configuración de la interfaz GigabitEthernet 0/1 en ambos switches, que ahora la tenemos definida como un enlace troncal que permite el paso de tramas de las VLAN 10 y 20. Por ejemplo, haremos lo siguiente en el Switch0 para eliminar la configuración actual:

```
Switch0#configure terminal
Switch0(config)#interface gigabitEthernet 0/1
```

```
Switch0(config-if)#no switchport mode trunk
Switch0(config-if)#no switchport trunk allowed vlan 10,20
Switch0(config-if)#exit
Switch0(config)#
```

Hay que hacer lo mismo con el otro switch. A continuación añadiremos un nuevo enlace que una las respectivas interfaces GigabitEthernet 0/2. Veremos que, tras hacer esto, este último cable añadido no consigue establecer una comunicación de manera satisfactoria a pesar de que el estado de la interfaz es up/up (círculo de color naranja).



La razón de ello es que el algoritmo STP (Spanning Tree Protocol) ha bloqueado la interfaz en el Switch1 para evitar bucles en la capa de enlace.

La creación de un enlace EtherChannel formado por dos cables implica que, a nivel interno del switch, se creará una única interfaz lógica (port-channel) que operará haciendo uso de las dos interfaces físicas. Si alguno de los dos cables se desconectara, la comunicación no se vería afectada ni tampoco se produciría un recálculo de las rutas definidas por el protocolo STP porque el enlace lógico seguiría operativo a través de las interfaces físicas restantes. Por lo tanto, el empleo de la tecnología EtherChannel no solamente permite un aumento del ancho de banda entre switches sino que, además, aumenta la confiabilidad del sistema de interconexión pues permite una cierta tolerancia a fallos.

En los conmutadores Cisco los puertos EtherChannel se identifican con el término port-channel y se les asigna un número que sirve para identificarlos. En nuestra topología llevaremos a cabo una configuración similar en ambos switches. En primer lugar se especifica que se usará el protocolo LACP, Link Aggregation Control Protocol (IEEE 802.3ad), para conformar el EtherChannel. En este caso es necesario que al menos uno de los dos extremos se defina en modo activo (active mode).

```
Switch0#configure terminal
Switch0(config)#interface range gigabitEthernet 0/1-2
Switch0(config-if)#channel-protocol lacp
Switch0(config-if)#channel-group 1 mode active
Switch0(config-if)#exit
```

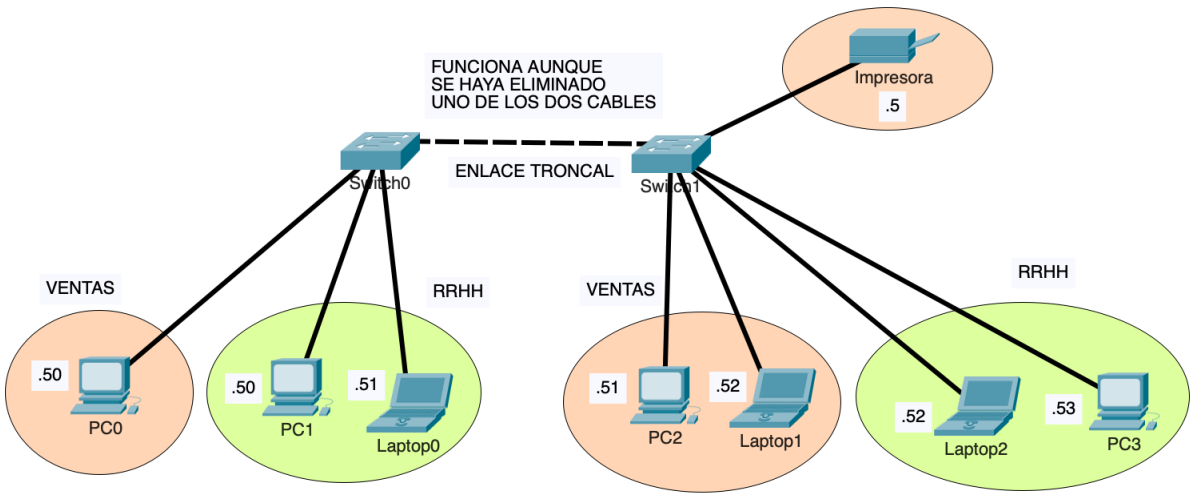
```
Switch0(config)#
```

Con esta configuración se ha definido el canal “port-channel 1” que comprende las dos interfaces físicas. Podemos hacer lo mismo en el otro switch (no sería necesario definirlo en modo activo porque ya lo está el anterior, y por otro lado, tampoco sería necesario asignarle el número 1 como identificador del port-channel).

En estos momentos veremos que los enlaces gozan de un estado up/up de forma conjunta como un canal de tipo EtherChannel. Sin embargo, todavía no podrá usarse en nuestra topología porque, salvo para la VLAN nativa, no permite tráfico de otras VLAN. Por tanto, ahora tendremos que configurar el enlace EtherChannel en modo troncal, igual que hicimos anteriormente con la interfaz GigabitEthernet 0/1, pero siguiendo la nomenclatura de Cisco lo haremos sobre el port-channel 1 como si de una interfaz física se tratara:

```
Switch0#configure terminal
Switch0(config)#interface port-channel 1
Switch0(config-if)#switchport mode trunk
Switch0(config-if)#switchport trunk allowed vlan 10,20
Switch0(config-if)#exit
Switch0(config)#
```

Después de hacer lo mismo en el otro switch veremos que ya es posible establecer la comunicación entre todos los hosts de la empresa. Se puede comprobar que esta comunicación se mantiene aunque uno de los enlaces físicos se elimine, aunque lo haría a 1 Gbps:

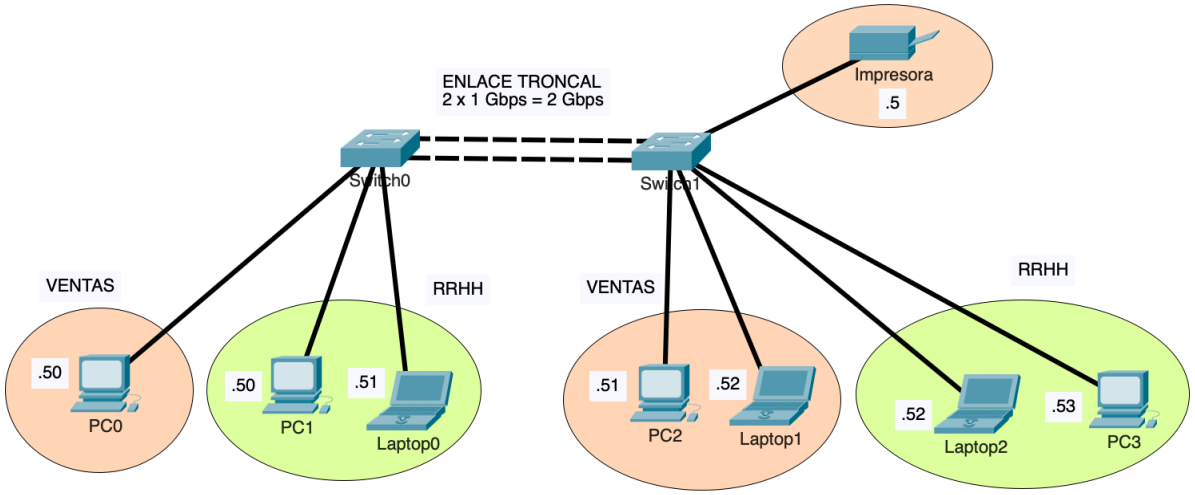


Bastaría con añadir el cable fallado para que el EtherChannel establecido recuperara el ancho de banda inicial (2 Gbps).

Instalación de una impresora: problemática

En último lugar, imaginemos ahora que se quiere incluir una impresora en la empresa. Esta impresora, necesariamente, deberá estar ubicada en una VLAN y también habrá de

disponer de configuración IP. Supongamos que la colocamos en el departamento de VENTAS y su dirección IP es 192.168.10.5.



Con la topología que hemos definido hasta este momento solo se permitirá el acceso a la impresora por parte de los hosts que están dentro de la VLAN del departamento VENTAS. Por ejemplo, desde PC0 tenemos conectividad:

```
C:\>ping 192.168.10.5

Pinging 192.168.10.5 with 32 bytes of data:

Reply from 192.168.10.5: bytes=32 time=1ms TTL=128
Reply from 192.168.10.5: bytes=32 time<1ms TTL=128
Reply from 192.168.10.5: bytes=32 time<1ms TTL=128
Reply from 192.168.10.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Sin embargo, si intentamos conectarnos a la impresora desde PC1 no podremos:

```
C:\>ping 192.168.10.5

Pinging 192.168.10.5 with 32 bytes of data:

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

Ping statistics for 192.168.10.5:
   Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Para poder compartir la impresora entre todos los departamentos hay que establecer algún mecanismo que permita circular la información a través tanto de VLAN como de redes IP

distintas. Este tipo de comunicación, como veremos más adelante, se puede llevar a cabo con la ayuda de un router o bien en switch de nivel 3.