SIMULACIÓN DE RED DE UNA EMPRESA.

Nerea Fdez Fernández

ÍNDICE

DISEÑO DE RED

1. Justificación técnica del diseño

Se ha construido una red usando VLANs, que básicamente son divisiones dentro de la red que ayudan a que todo funcione mejor, sea más seguro y fácil de administrar. La idea es separar el tráfico de acuerdo a su función, para evitar colisiones y tener mejor control sobre cada tipo de dispositivo. La empresa es de tamaño medio, pero también se ha tenido en cuenta que la red pueda crecer sin problemas en el futuro. Esto significa que se pueden añadir nuevas VLANs, más equipos o servicios a medida que la empresa crezca.

Estructura actual de la empresa:

- **VLAN 10 (ORDENADORES):** para tareas administrativas y de gestión.
- **VLAN 20 (IMPRESORAS):** donde se comparten las impresoras entre diferentes departamentos.
- **VLAN 30 (WIFI):** punto de acceso para portátiles.
- **VLAN 40 (ROUTER):** para comunicación y salida a internet.

Este diseño modular no solo hace que la red sea más segura y eficiente, sino que también facilita el mantenimiento, la supervisión y la puesta en marcha de políticas de la red. Cada VLAN se puede administrar por separado, y lo mejor es que permite agregar nuevas tecnologías o departamentos en el futuro, sin tener que hacer cambios grandes en la estructura existente. Así, la red está preparada para seguir creciendo sin complicaciones.

DISEÑO DE RED

2. Topología, tipo de red y medios de transmisión

- **Topología lógica:** He utilizado una topología en estrella por su facilidad de gestión, posibilidad de ampliación y tolerancia a fallos, ya que si un nodo falla, no afecta al resto de la red. En el centro de la red se ha colocado un switch de capa 3, que actúa como el cerebro de la red, ya que permite la gestión de VLANs y el enrutamiento entre ellas sin necesidad de un router adicional, lo cual mejora el rendimiento y la eficiencia general del sistema.
- **Topología física:** La arquitectura física se organiza en un armario rack centralizado donde se ubican los dispositivos principales de red, como el switch de capa 3 y el router. Desde este punto, se distribuyen las conexiones hacia los distintos dispositivos finales.

Dispositivo	Tipo de conexión	Descripción
Hosts (ordenadores de sobremesa)	Cableado Ethernet	Conectados directamente al switch.
Impresoras de red	Cableado Ethernet	Conectadas al switch mediante cable.
Punto de Acceso (AP)	Cableado Ethernet	Ubicado estratégicamente, conectado al switch para ofrecer cobertura WiFi.
Portátiles	Conexión inalámbrica (WiFi)	Se conectan al AP mediante sus adaptadores de red inalámbricos.
Router	Cableado Ethernet	Conectado al switch para permitir acceso a Internet o a otras redes externas.

- **Tipo de red:** Se trata de una red LAN (Red de Área Local), segmentada mediante VLANs para organizar y separar el tráfico según necesidades específicas.
- **Medios de transmisión:** Se utilizan cables Ethernet de par trenzado de categoría 6 para las conexiones cableadas entre el switch y los dispositivos como ordenadores, impresoras, AP y router.

CONFIGURACIÓN DE RED

3. Configuración de red

VLAN	Dispositivos	Rango IP
10	**Hosts**	192.168.10.0/24
20	**Impresoras**	192.168.20.0/24
30	**Portátiles**	192.168.30.0/24
40	**Router**	192.168.40.0/24

- Estas han sido creadas en el apartado Config del Switch, en Switching "VLAN Database".

  VLAN Number: N° de la VLAN.
  VLAN Name: Nombre de la VLAN.

Una vez creadas, todavía no estarían funcionales. Para que puedan operar correctamente en la red, es necesario asignar una interfaz para cada VLAN con su respectiva IP. Como mostraré a continuación:

- **El Switch capa 3 tiene configuradas las siguientes interfaces:**

  - **interfaz vlan 10 →** IP 192.168.10.1
  - **interfaz vlan 20 →** IP 192.168.20.1
  - **interfaz vlan 30 →** IP 192.168.30.1
  - **interfaz vlan 40 →** IP 192.168.40.1

Esto se ha hecho configurando las interfaces en el switch mediante comandos:

Nos iremos al apartado CLI del switch y pondremos lo siguiente:

```
Enable
Configurate terminal
Interface vlan 10
Ip address 192.168.10.1 255.255.255.0
No shutdown
Exit
```

Esto se hará sucesivamente con todas las VLANs con sus respectivas IP.

- El router está conectado a: GigabitEthernet0/1 y configurado con la IP 192.168.40.10.

CONFIGURACIÓN DE RED

4. Configuración de adaptadores de Red.

PC de Sobremesa:

- Abrimos el PC, y en la pestaña “Settings” en el Gateway añadiremos la IP de su respectiva Vlan 192.168.10.1
- Luego nos iremos a la pestaña FastEthernet0, le daremos clic a Static en el IPv4 y añadiremos la IP correspondiente con su máscara.
- Apagamos y encendemos.

Impresora:

- Parecido al PC, en la pestaña “Settings” en el Gateway añadiremos la IP de su respectiva Vlan 192.168.20.1
- Luego nos iremos al FastEthernet0 y lo mismo, daremos clic a Static en el Ipv4 y añadiremos la IP correspondiente con su máscara.
- Apagamos y encendemos.

Punto de Acceso:

- 1. Nos iremos al apartado de Config, y en el Port 1, añadiremos las configuraciones necesarias.
- 2. Port Status (nombre que le daremos al punto de acceso): wifi
- 3. Authentication: WPA2-PSK (para mayor seguridad, ya que tiene cifrado AES).
- 4. En el PSK Pass Phrase (pondremos la contraseña): prueba1234.
- 5. Apagamos y encendemos.

Portátiles:

- En el apartado Physical (físico), quitaremos el módulo de cableado y pondremos el WPC300N (para conexión inalámbrica).
- Nos iremos a la pestaña Settings en Config, y en Gateaway añadiremos la IP de su respectiva Vlan 192.168.30.1
- Luego nos iremos a la pestaña Wireless0 y le damos a Static en IPv4, y añadiremos la IP correspondiente con su máscara.
- En el SSID, añadiremos el nombre que le dimos al punto de acceso “wifi” y en el PSK Pass Phrase la contraseña: prueba1234.
- Luego para conectarlo, nos iremos a “Deskpot” y al apartado “PC Wireless”, una vez dentro en el apartado de Connect, le daremos a refresh y nos debería salir el punto de acceso, lo señalamos y le damos a connect

Router:

- Nos iremos a config y en la pestaña GigabitEthernet0/1 asignaremos su correspondiente IP 192.168.40.10 con su máscara 255.255.255.0

CONFIGURACIÓN DE RED

5. Integración de Dispositivos

- **VLAN 10 (ORDENADORES):** 11 hosts conectados por cable, con IPs desde 192.168.10.10 a 192.168.10.20.
- **VLAN 20 (IMPRESORAS):** 3 impresoras por cable, IPs 192.168.20.10-12.
- **VLAN 30 (WIFI):** 1 punto de acceso por cable, conectando 3 portátiles mediante tarjeta de red con IPs 192.168.30.10-12.
- **VLAN 40 (ROUTER):** Router con IP 192.168.40.10 conectado a GigabitEthernet0/1.

Para facilitar la identificación visual en el switch, se aplicó un color distinto a los dispositivos según su VLAN en la red. Además, se asignaron los siguientes puertos del switch:

Puerto del Switch	Dispositivo	VLAN Asignada
Fa0/1 – Fa0/11	Hosts	VLAN 10
Fa0/12 – Fa0/14	Impresoras	VLAN 20
Fa0/15	Punto de Acceso (AP)	VLAN 30
GigabitEthernet0/1	Router	VLAN 40

Una vez creadas las VLANs y configuradas las IPs correctamente, procedí a establecer los puertos de entrada en el switch con los siguientes comandos:

Nos iremos al apartado de CLI del Swtich y pondremos lo siguiente:
Enable
Configure terminal
Interface range fastEthernet 0/1 – 11 (Tendremos que ir de uno en uno).
Switchport Access vlan 10
No shutdown (Esto es para que no se apague).
Exit

Esto se hará igual, con las impresoras y con el punto de acceso, solo que cada una con su respectivo puerto y vlan correspondiente. Ahora bien, el procedimiento para el WiFi es diferente, por ello procederé a explicarlo a continuación:

CONFIGURACIÓN DE RED

5. Integración de Dispositivos

En la misma pestaña CLI del Switch pondremos lo siguiente:
Enable
Configure terminal
Interface gig0/1
Switchport mode Access
Switchport Access vlan 40
No shutdown
Exit

Con esto habríamos habilitado el router al puerto del switch, pero nos faltaría ahora que el router pueda comunicarse con el switch en la VLAN 40. Por ello nos iremos a la configuración del router, y en la pestaña CLI pondremos lo siguiente:

Enable
Configure terminal
Ip route 192.168.0.0 255.255.0.0 192.168.40.1 (esto permitirá la comunicación con el switch en la VLAN 40 y a parte ser vista por toda la red).
No shutdown
Exit

Más adelante gestionaremos ACL (Listas de control de Acceso) para que sea más segura la red.

6. Verificación de Conectividad

Para asegurarme de que la red funciona correctamente, realicé pruebas de **ping** desde cada dispositivo:

- A la IP de la VLAN.
- A otros dispositivos, según las reglas de acceso entre VLANs.
- Al router (192.168.40.10).

Desde el switch de capa 3, usamos comandos como **show ip interface brief** para comprobar el estado de las interfaces, y se hacen **pings** de prueba para verificar el enrutamiento entre VLANs.

MONTAJE Y COMPROBACIÓN

7. Tipo de cables utilizados

- **Cables directos (straight-through):** entre PCs, impresoras y el switch.
- **Conexiones inalámbricas:** mediante tarjetas de red de los portátiles hacia el AP (Access Point).

8. Conectores

Se utilizaron conectores RJ-45 estándar para todos los dispositivos Ethernet.

9. Comprobación de conectividad

- Con ping entre dispositivos.
- Y con verificación visual del estado de los cables en el switch, los LEDs, están todos en verde parpadeando, significando una conexión activa.

ADMINISTRACIÓN DE RED

10. Configuración avanzada del Switch

A continuación, procederemos a crear las ACL (Listas de control de acceso) en el Switch.

Objetivo:

- Que el punto de acceso VLAN 30, no vea ni a la VLAN 10 ni a la VLAN 20.
- Todas las VLANs podrán comunicarse con el router (VLAN 40).
- VLAN 10 y 20 sí pueden comunicarse entre sí y con VLAN 40, pero no con el VLAN 30.

La VLAN 30 está reservada para dispositivos WiFi, como los portátiles. La idea de separarla del resto es para proteger los recursos internos y la información confidencial de las estaciones de trabajo con cable. Esta separación crea una red como la que usan las empresas, donde se controlan mejor los accesos desde redes inalámbricas menos seguras. Ahora, explicando esto, paso a la configuración:

ADMINISTRACIÓN DE RED

10. Configuración avanzada del Switch

Para ello nos iremos al switch y en el apartado CLI comenzaremos a escribir:

Enable
Configure terminal
ip access-list extended FILTRO_WIFI
deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255 (Bloquea el tráfico de la VLAN 30 a VLAN 10).
deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
permit ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255 (Permite el tráfico del VLAN 30 al VLAN 40).
Exit

Ahora haremos lo mismo, pero bloqueando el tráfico de la VLAN 10 y 20 a la VLAN 30:

Enable
Configure terminal
ip access-list extended WIFI_FILTRO
deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
permit ip any any
exit

Una vez listo aplicaremos las ACL en las VLANs:

interface vlan 10
ip access-group WIFI_FILTRO out
interface vlan 20
ip access-group WIFI_FILTRO out
interface vlan 30
ip access-group FILTRO_WIFI out

La VLAN 40 está diseñada como red de gestión y salida a internet, por lo que no tiene restricciones en las ACL y puede comunicarse libremente con las demás VLANs. Al no aplicarse ninguna ACL en la interfaz VLAN 40, el tráfico entrante y saliente no se filtra, permitiendo así que funcione como punto central de acceso y gestión.

ADMINISTRACIÓN DE RED

11. Gestión de la tabla MAC

- Verificaremos la tabla MAC en el switch con el siguiente comando: **show mac address-table**, también podemos usar el comando **show ip arp** (lista de MACs conectados al switch).

- La tabla MAC muestra qué dispositivos están conectados a qué puerto del switch.

12. Seguridad de puertos

Para aplicar una capa de seguridad a los puertos, realizaremos los siguientes comandos en el Switch (CLI):

Enable
Configure terminal
Interface range fa0/1 - 11
Switchport mode access
Switchport port-security
Switchport port-security maximum 1 (esto indicará que solo puede haber un dispositivo en cada puerto)
Switchport port-security violation restrict
Switchport port-security mac-address sticky
Exit

Haremos lo mismo con los puertos de la impresora. Ahora bien, para el punto de acceso, al tener conexiones inalámbricas de 3 portátiles tendremos que añadir un máximo de 3 dispositivos conectados. Estas restricciones en caso de ser necesario ampliar, se podrán modificar más adelante sin problema.

Enable
Configure terminal
Interface range fa0/15
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security mac-address sticky
exit

ADMINISTRACIÓN DE RED

13. STP y modificación del puente raíz

Qué hace el STP:

- Detecta topologías redundantes.
- Elige un Root Bridge (switch raíz).
- Bloquea puertos para prevenir bucles.
- Recalcula automáticamente si un enlace falla.

Sabiendo esto, lo que haremos será configurar las VLANs como puente raíz, para ellos nos iremos al Switch en el apartado CLI e escribiremos los siguientes comandos:

spanning-tree vlan 10 priority 24576
spanning-tree vlan 20 priority 24576
spanning-tree vlan 30 priority 24576
spanning-tree vlan 40 priority 24576

Esto permitirá a cada VLAN ejecutar su propia instancia de STP (ya que están aisladas), por lo que podemos tener uno distinto para cada VLAN.

14. Monitorización con SNMP

Para utilizar el SNMP, y monitorizar la red, nos iremos al router al apartado CLI y procederemos a usar los siguientes comandos:

Enable
configure terminal
snmp-server community read ro
snmp-server community write rw
exit

Desde un PC accederemos al apartado Deskpot y nos iremos al MIB Browser, allí nos iremos a advanced y meteremos los siguientes datos:

Address: **192.168.40.10**
Port: **161 (viene por defecto)**
Read Community: **read (el nombre que dimos antes en el router)**
Write Community: **write (lo mismo aquí)**
SNMP Version: **V3**
OID: **1.3.6.1.2.1.1.5.0 (nombre del router)**

Este lo encontraremos en el apartado system, en sysName, nada mas darle cogerá el OID y al darle al GO te saldrá el nombre “router” (Valor), ID, Tipo, etc. También podemos mirar el tiempo activo y mucho más.

CONCLUSIÓN

En resumen, este diseño de red permite una segmentación eficiente mediante el uso de VLANs, mejora la seguridad con listas de control de acceso (ACLs) y otras medidas como STP, seguridad en puertos y SNMP. Además, está pensado para ser escalable y fácil de administrar gracias a su estructura jerárquica. La configuración del puente raíz también aporta mayor disponibilidad a la red. Todo el proceso ha podido ser simulado, verificado y documentado con precisión gracias a Cisco Packet Tracer.

BIBLIOGRAFÍA

Estructura de red, Mapa físico y lógico
https://youtu.be/26H5mbZbxLc?si=amfkueEMNh6izMaJ

VLANs
Tutorial: Configurar una VLAN con Packet Tracer | Marcos Ruiz
▷ Configuración de VLANs en Packet Tracer

STP
Comandos para configurar stp en packet tracer - Mundowin

Configuración SNMP
https://youtu.be/t8GQYxQeuE0?si=qvmHulS1lV5BG2Sb
SNMP Commands

General
Configuración del uso de puente transparente - Cisco