Unidad 6

Configuración de redes virtuales VLANs

Planificación y Administración de Redes

Índice

Introducción

Aunque el uso de los primeros switches hizo que el rendimiento de las LAN se viera francamente incrementado, para grandes estructuras de red, surgen nuevos problemas que hacen que el rendimiento se vuelva a ver afectado.

Se crean, basándonos en el envío de los mensajes de difusión, los protocolos TCP/IP, que se pueden usar para desde asignar una dirección IP hasta para enviar un archivo.

El trabajo de un switch consiste en el envío de todas estas tramas de difusión a través de todos los puertos disponibles menos el de origine, generando mucho tráfico. Se usa el protocolo STP para que no se creen bucles, pero no elimina los cuellos de botella, lo que como hemos dicho, puede causar que haya problemas de rendimiento.

Para que, además, haya una correcta administración y aseguramiento de la información, habrá zonas de la organización que deban estar asiladas de otras, menos para información en común.

Para poner solución a estos impedimentos tenemos dos opciones:

- El uso de routers para separar cada una de las subredes.
- El uso de switches que puedan crear VLANs.

Al finalizar esta unidad

- Sabremos lo que son las redes virtuales.
- Conoceremos como son las tramas de las VLANs
- Distinguiremos los distintos tipos de VLAN según membresía, enlaces y funciones.
- Podremos configurar redes virtuales en switches CISCO.
- Seremos capaces de configurar dinámicamente las VLANs con el protocolo VTP.
- Conoceremos el diseño de las redes jerárquicas, sus capas, ventajas y principios.

6.1. VLAN. Red LAN virtual

6.1.1. Concepto de VLAN

Lo primero que vamos a hacer en esta pequeña introducción es distinguir entre dominio de colisión y dominio de difusión:

- **El dominio de colisión** está formado por un conjunto de equipos que se encuentran conectados entre ellos por *hubs* o cables directos, compartiendo todos los equipos el medio que actúa de bus lógico.

  Los *switches*, *bridges* y *routers* se usan para separar los dominios de colisión.

- **El dominio de difusión** está formado por un conjunto de equipos conectados mediante hubs, bridges y switches.

  Para hacer una segmentación o separación entre distintos dominios de difusión, se usan los *routers*, ya que los mensajes de difusión no pueden pasar de uno s a otros. Estos mensajes son los que se mandan a toda una misma subred, es decir, a la dirección de difusión de la red.

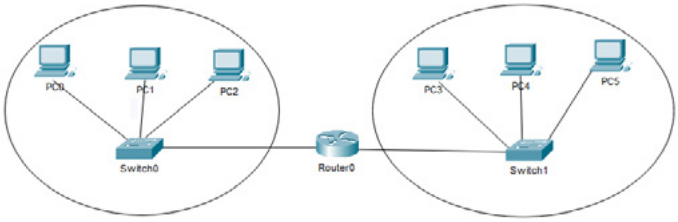

Imagen 1. Dominios de difusión

Una VLAN es un mecanismo que da la oportunidad a los *switches* gestionables de separar la red en distintos dominios de difusión sin necesidad de usar *routers* intermedios, ya que estos últimos son más lentos.

En un ejemplo tenemos una VLAN para informática (INF), y otra para marketing (MKT), con distintos equipos. En cada VLAN tenemos un distinto dominio de difusión por lo que cada mensaje de difusión que se mande se aplicará para todos los equipos de la VLAN.

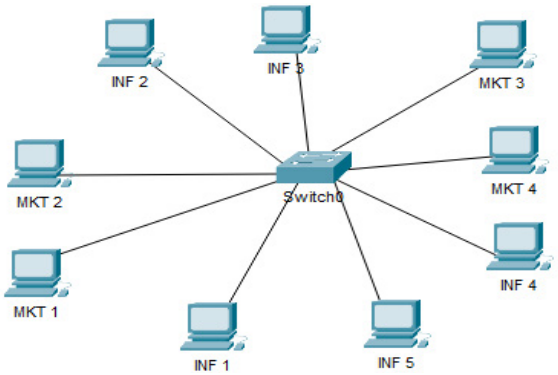

Imagen 2. Dos VLAN con los equipos en el mismo segmento de una red

De manera más clara, podemos separar físicamente y por segmentos los equipos de las VLANs, como en la siguiente imagen:

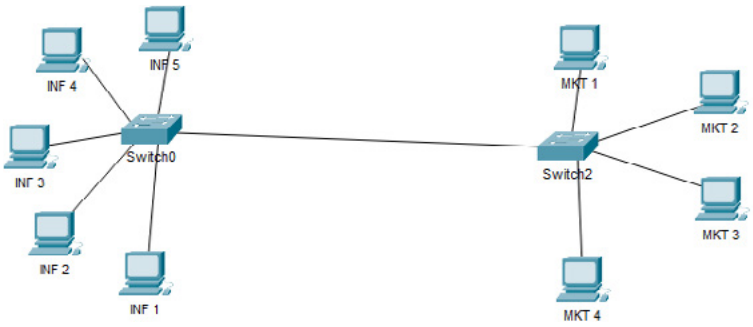

Imagen 3. Dos VLAN con los equipos en distintos segmentos de una misma red

6.1.2. Formato de trama IEEE 802.1q para VLAN

Cuando queremos crear una VLAN, lo que debemos de hacer es asignar etiquetas a las tramas Ethernet añadiendo además algo de información, que son los dos nuevos campos, *EtherType* y TCI.

Mientras que *EtherType* tiene el valor 0x8100, que significa que se tratad e una trama lista para una VLAN, TCI, se divide en 3 subcampos:

- *Priority* que indica cual es la prioridad del tráfico y además se usa para la transmisión de voz y multimedia.
- CFS que es el indicador de formato canónico.
- *VLAN ID para identificar la VLAN de destino.*

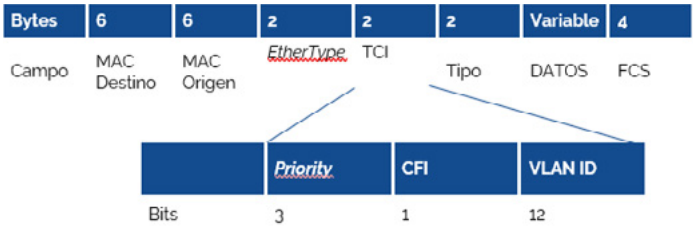

Imagen 4. Formato de trama IEEE 802.1Q para VLAN

6.1.3. Tipos de VLAN según membresía

Si no tenemos claro que mecanismo usar para la asignación de los miembros de una VLAN, las redes virtuales se pueden clasificar en:

- VLAN por puerto o de nivel 1.
- VLAN por dirección MAC o de nivel 2.
- VLAN por dirección IP o de nivel 3.

VLAN de nivel 1 por puerto

Se determina que equipo está en cada VLAN dependiendo del puerto al que esté conectado. Esta configuración, aunque valida, presenta el inconveniente de que si cambiamos algún equipo de puerto, habría que cambiar la configuración para que siga perteneciendo a la misma VLAN.

Es el tipo de VLAN más usado y el que usaremos en nuestros ejemplos.

VLAN de nivel 2 por dirección MAC

Se determinan los miembros de una VLAN dependiendo de su dirección MAC o física.

VLAN de nivel 3 por dirección IP

Se determinan los miembros de una VLAN dependiendo de su dirección IP de red.

6.1.4. Tipos de enlaces

Si tenemos el *switch* conectado a un dispositivo con capacidad de reconocer las VLAN o no, los tipos de enlace son o de acceso o troncales.

Enlace de acceso

También se le puede llamar *Access Link*.

El *switch* gestionable se encuentra conectado a un dispositivo que **NO** reconoce el funcionamiento mediante las VLANs creadas. Un ejemplo podría ser un *switch* conectado a una impresora.

Las tramas que van a ir pasando `por este enlace deben de **no** etiquetarse porque pertenecen siempre a la misma VLAN. Los puertos que conecten con los enlaces en los dispositivos también deben de estar como no etiquetados.

Enlace troncal

Este tipo de enlace conecta dos dispositivos que reconocen los estándar VLAN, y son llamados *Trunk Link*. Se puede dar, por ejemplo, entre dos *routers*.

En este enlace puede que pasen tramas de distintas VLANs, por lo que todas deben de estar correctamente etiquetadas.

Si el enlace troncal se usa para *switches*, puede que se encuentre formado por más de un único cable, debiendo configurarse para que el ancho de banda quede repartido entre los que sean, para poder tener una mayor velocidad de transmisión.

6.1.5. Tipos de VLAN según su función

VLAN Predeterminada

Estas son las VLAN a las cuales se les asignan todos los puertos de un *switch* cuando iniciamos el dispositivo.

Para los *switches* CISCO, esta es por defecto la VLAN 1.

VLAN de Datos

Se tratan de las VLAN que solo se usan, porque su configuración así está establecida, para enviar el tráfico de datos generado únicamente por el usuario, por lo que también se la denomina VLAN de usuario.

VLAN de administración

Las VLAN de administración están configuradas para que el administrador pueda realizar tareas de gestión en el *switch*. LA VLAN 1 puede servir por defecto para este tipo de tareas, aunque es conveniente que se cambie por otra, que suele ser la VLAN 99.

VLAN Nativa

LA VLAN nativa es la que se encuentra asignada a un puerto del enlace troncal y que están asignada a este puerto antes de que se estableciera dicho enlace. Esta VLAN, puede ser modificada después mediante comandos del *switch*. Aunque esta VLAN sirve a modo de identificador común en los extremos opuestos del enlace troncal, es aconsejable que no usemos la VLAN 1 como la VLAN nativa.

Según el modo de trabajo de un puerto

Dependiendo del modo de trabajo del puerto,los tipo de VLAN son:

- **VLAN estática.** Cada uno de los puertos del *switch* están automáticamente asignados a una VLAN.

Imagen 5. VLAN estática

- **VLAN dinámica.** En este caso se configura la membresía de una VLAN usando un servidor que llamamos VMPS o Servidor de Política de Membresía de VLAN.

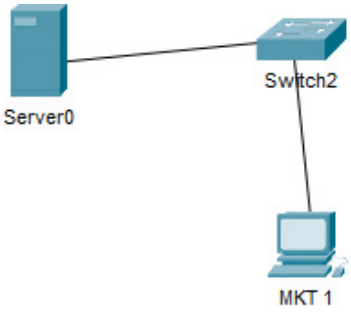

Imagen 6. VLAN dinámica

- **VLAN de voz.** Es la VLAN en las que el puerto se configura en modo de voz para poder conectarlo a un teléfono IP. En varias ocasiones, el teléfono funciona a modo de *switch* para que, si conectamos un equipo, reciba señal, funciona como un intermediario en el *switch* gestionable y el terminal final.

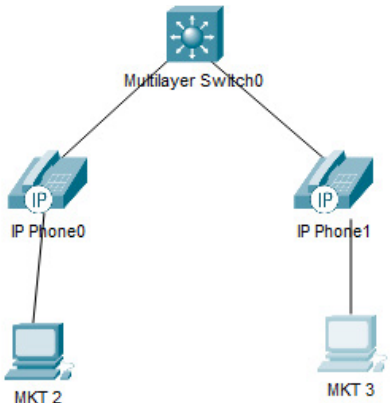

Imagen 7. VLAN de voz

6.1.6. Comandos Cisco para gestión de VLAN

- Para crear una VLAN:

  1. Lo primero que hacemos es ingresar en el *switch*, habilitarlo y entrar en modo configuración.
  2. Después lanzamos el comando:

     ```
     vlan vlan_id
     ```

  3. Automáticamente, nos entrará en el modo de configuración de la VLAN, y si queremos asignarle un nombre usamos el comando:

     ```
     name nombre_vlan
     ```

  4. Salimos de la configuración.

```
Switch(config)#
Switch(config)#vlan 7
Switch(config-vlan)#name ASIR
Switch(config-vlan)#exit
Switch(config)#
```

Imagen 8. Crear VLAN en Cisco

- Para eliminar la VLAN creada anteriormente, lanzamos el comando:

  ```
  no vlan vlan_id
  ```

  Cuando se elimina una VLAN, es necesario eliminar también un archivo llamado *VLAN.dat* que se crea en el *switch*, en la memoria *flash* y contiene la información de la base de datos de la VLAN, si no lo borramos, tenemos el problema de que al reiniciar el *switch* la VLAN volverá a aparecer. Para eliminarlo, lanzamos el comando:

  ```
  delete flash:vlan.dat
  ```

  Y damos *ENTER* en las dos siguientes preguntas de confirmación.

```
Switch(config)#
Switch(config)#no vlan 7
Switch(config)#
```

Imagen 9. Eliminar VLAN en Cisco

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
```

Imagen 9. Borrar archivo de configuración de VLAN en Cisco

- Para configurar un enlace de acceso, seguimos los pasos siguientes:

  1. Entramos en el modo de configuración de la interfaz que deseemos.
  2. Usamos el comando:

     ```
     switchport access vlan vlan_id
     ```

  3. Salimos del modo de configuración de la interfaz.

```
Switch(config)#
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport access vlan 7
Switch(config-if)#exit
Switch(config)#
```

Imagen 10. Enlace de acceso en Cisco

- Si queremos configurar un enlace troncal, realizamos el proceso siguiente:

  1. Entramos en la configuración de la interfaz elegida.
  2. Lanzamos el comando:

     ```
     switchport mode trunk
     ```

3. Salimos de la configuración.

```
Switch(config)#
Switch(config)#interface FastEthernet1/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#
```

Imagen 11. Enlace troncal en Cisco

> Para ver las VLAN que tenemos en forma de tabla:

```
show vlan [brief]
```

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active    Fa1/1, Fa2/1,
Fa3/1, Fa4/1
                                                Fa5/1
7    ASIR                             active    Fa0/1
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

Imagen 12. Tabla de VLAN en Cisco

> Si queremos mostrar en pantalla el estado y las estadísticas de los puertos:

```
show interfaces [nombre_puerto] [switchport]
```

```
Switch#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 7 (ASIR)
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: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
```

Imagen 13. interfaces del *switch*

En este caso, saldrían todos los puertos y algo más de información, pero solo ponemos una imagen debido a la longitud tan extensa de esta salida.

> Por último, para ver la configuración de los puertos troncales:

```
show interfaces trunk
```

```
Switch#show interfaces trunk
```

Imagen 14. Puertos troncales

EJEMPLO

Nos encontramos con dos aulas y en este caso, dos equipos en cada una de ellas.

En el aula **ASIR**, tenemos la red 192.168.1.0/24, los equipos deben tener una ip fija, la cual será:

Nombre	Ip equipo	Máscara	Gateway	VLAN
PC0	192.168.1.2	255.255.255.0	192.168.1.1	10
PC1	192.168.1.3	255.255.255.0	192.168.1.1	10
Switch1				10 y 30

Podemos darle el nombre que queramos a los equipos, al igual que el nombre a la VLAN, en este caso hemos utilizado el nombre VLAN10.

En el aula **MULTIPLATAFORMA**, tenemos la red 192.168.2.0/24

Nombre	Ip equipo	Máscara	Gateway	VLAN
PC2	192.168.2.2	255.255.255.0	192.168.1.1	20
PC3	192.168.2.3	255.255.255.0	192.168.1.1	20
Switch2				20 y 30

Una vez tenemos establecida la distribución, **añadiremos a los equipos** la dirección IP y sobre todo la dirección de la puerta de enlace. Que será distinta en cada aula.

Configuración en los *switches*

La configuración de los switches es muy sencilla y la trataremos a través de comandos. Pondremos todos las conexiones (en este caso, 2 equipos) en la misma VLAN y para ello haremos lo siguiente:

> Switch1:

```
Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name VLAN10
Switch(config-vlan)#int r f0/1-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#
```

Imagen 15. Ejemplo VLAN 3

> Switch2:

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 20
Switch(config-vlan)#name VLAN20
Switch(config-vlan)#int r f0/1-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#
```

Imagen 16. Ejemplo VLAN 4

- **Switch3:**

  La configuración de este switch central es más extensa porque este es el encargado de diferenciar las distintas VLAN a la vez que se comunica con el *router*.

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name VLAN10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name VLAN20
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name VLAN30
Switch(config-vlan)#int f0/24
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access v
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/24 (1),
with Switch FastEthernet0/24 (10)
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/23 (1),
with Switch FastEt
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int f0/23
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#int f0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport nonegotiate
Switch(config-if)#switchport access vlan 30
Switch(config-if)#
```

Imagen 17. Ejemplo VLAN 5

Configuración del *router*

Bien, muy bien, ya tenemos los 3 switches configurados y casi nuestra red ya está operativa para que los alumnos puedan estudiar.

Nos queda configurar el *router*, lo haremos con 2 interfaces virtuales con la IP correspondiente.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int f0/0.10
Router(config-subif)#encapsu
Router(config-subif)#encapsulation dot
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip add 192.168.1.1 255.255.255.0
Router(config-subif)#no sh
Router(config-subif)#int f0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip add 192.168.2.1 255.255.255.0
Router(config-subif)#no sh
Router(config-subif)#
```

Imagen 18. Ejemplo VLAN 6

Una vez terminado esta configuración, levantaremos la red con:

```
Router(config)#int f0/0
Router(config-if)#no sh

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed state to up
```

Imagen 19. Ejemplo VLAN 7

Comprobación

Para poder terminar, realizaremos un ping desde un equipo de un aula a otro equipo.

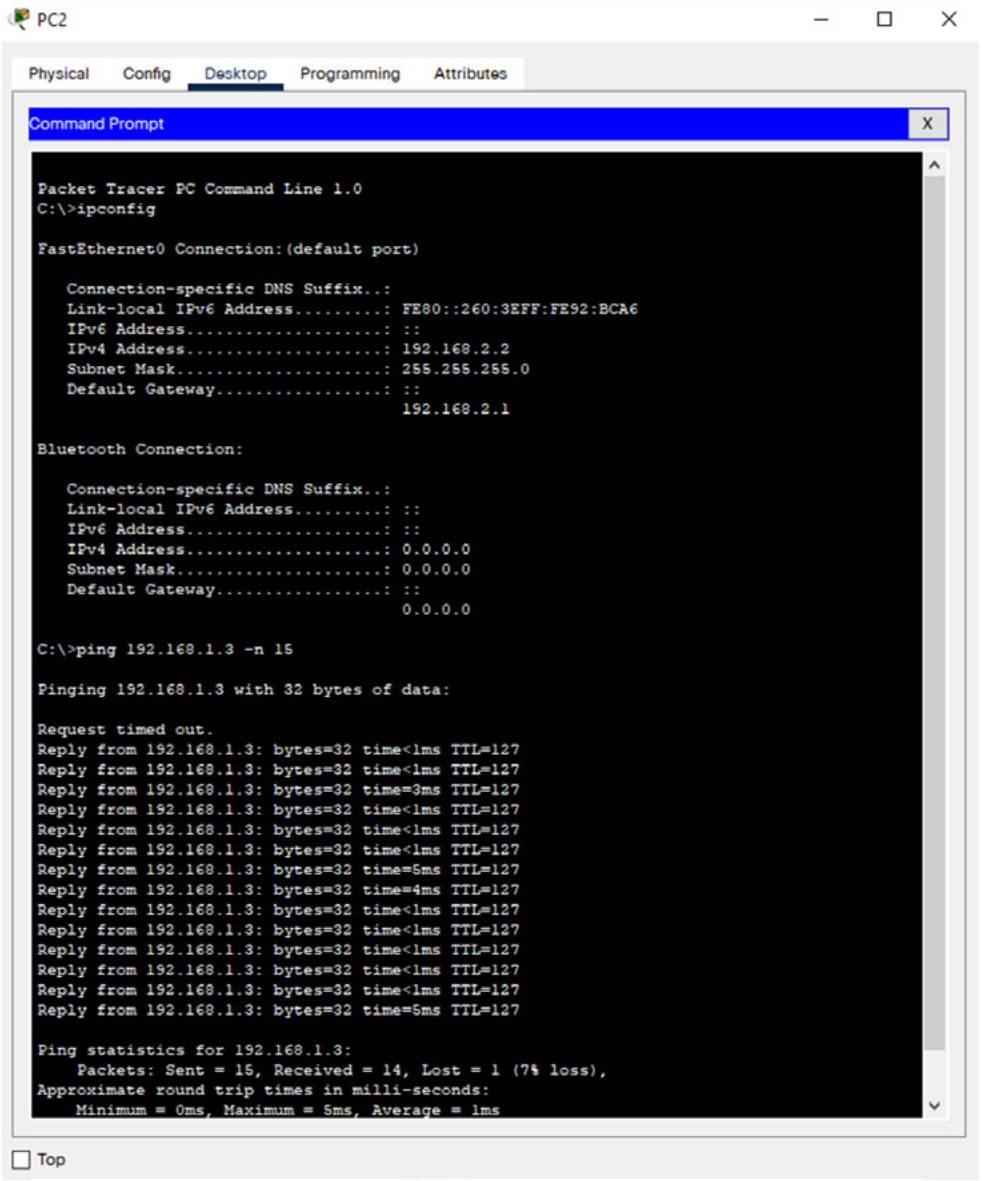

Imagen 20. Ejemplo VLAN 8

6.2. Protocolo VTP. Configuración dinámica de VLANs

El protocolo *VLAN Trunking Protocol*, cuyas siglas son VTP es el usado para la asignación a diversos *switches* de la configuración de *VLANs* desde un *switch* principal que usamos a modo de servidor. Con esto, lo que conseguimos es tener la administración centralizada de manera única en un único *switch* con la base de datos de todas las *VLANs*.

6.3. Diseño de una red jerárquica

6.3.1. Capas de una red jerárquica

Cuando tenemos una empresa más o menos pequeña o de mediano tamaño, lo mejor que podemos hacer es diseñar su red de **modo jerárquico**. Las redes jerárquicas se basan en capas distintas e independientes de la red para que cada una cumpla con su función y así, hacer más fácil la administración y corrección de errores. Por lo general, el modelo jerárquico de las redes cuenta con tres capas, **la de acceso, la de distribución y la de núcleo.**

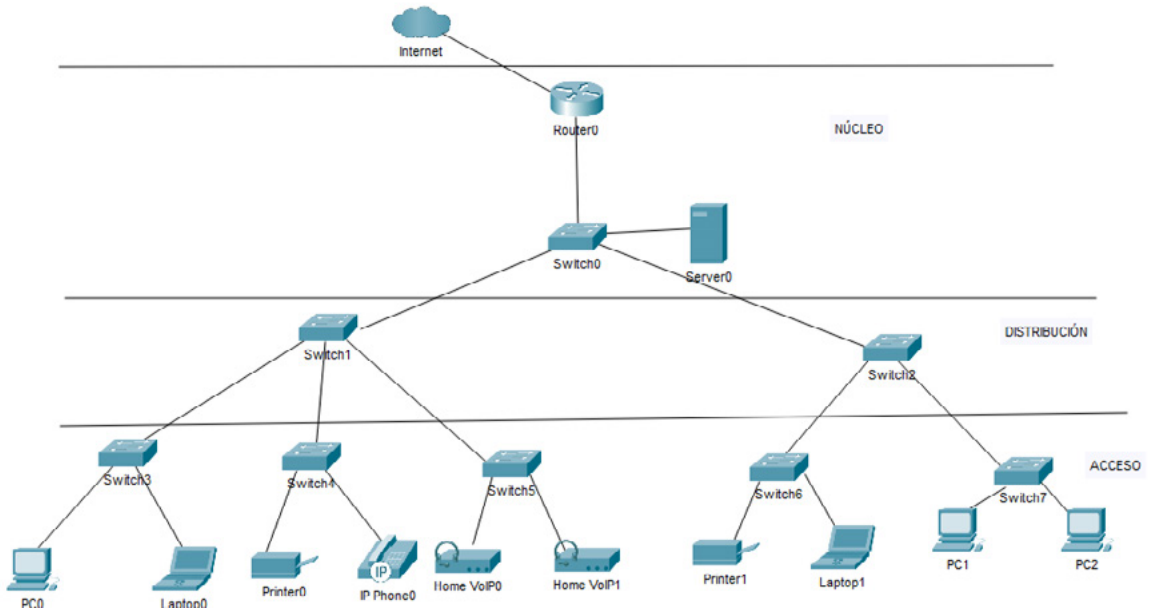

Imagen 21. Red jerárquica

Capa de acceso

Esta sería la capa más cercana al usuario final, ya que conectar con los dispositivos finales de la conexión como los equipos de sobremesa, dándoles acceso a Internet. En esta capa puede que nos encontremos con *routers, switches*, y demás dispositivos de interconexión de redes. La función principal de esta capa, como hemos dicho antes, es dotar de acceso a la red a los dispositivos de esta, crear el medio.

Capa de distribución

La capa de distribución funciona a modo de intermediaria entre la capa de acceso y la capa núcleo. En esta capa se procede a controlar el tráfico de todas las tramas que pasan por aquí ayudándose de políticas y protocolos. Además, aquí se determina el dominio de difusión al realizar el enrutamiento entre las *VLANs* que se hayan definido en la capa anterior. En esta capa solo nos encontramos con dispositivos de interconexión, por lo general solo *switches*, que deben de presentar alta disponibilidad y fiabilidad.

Capa núcleo

La capa de núcleo debe de ser la capa que goce de las mayores prestaciones de la vez ya que es una capa que necesita mucha velocidad. Esta capa también tiene conexión a internet y se encarga que transportar todo el tráfico heredado de la capa de distribución hacia internet, por esto la necesidad de las altas prestaciones.

6.3.2. Ventajas del diseño de red jerárquico

Escalabilidad

Como se trata de un diseño modular, las redes jerárquicas pueden aumentar su tamaño de manera relativamente fácil, al poder reproducir de manera casi exacta los elementos agregados a la red.

Redundancia

Los *switches* que tenemos disponibles en la capa de acceso se pueden conectar con dos o más *switches* correspondientes a la capa de distribución, y de igual modo los de la capa de distribución con los de núcleo.

En la capa de acceso es en la única en la que no tenemos redundancia porque si falla alguno de los dispositivos de interconexión, se desconectan solo los equipos o dispositivos que dependen de este, los equipos finales.

Rendimiento

Como los enlaces y los *switches* que encontramos en la capa de núcleo son de alto rendimiento, nos permiten que se obtenga la velocidad máxima de la red en casi su totalidad, siempre teniendo en cuenta la capacidad del cable que usemos.

Seguridad

En la capa de acceso tenemos la opción de configurar los *switches* con el modo de seguridad de puerto, `para poder decidir que dispositivos pueden conectarse a la red y cuáles no.

Además, como comentamos anteriormente, en la capa de distribución existen políticas de control de acceso implantadas que nos permiten realizar un filtrado del tráfico siguiendo protocolos de alto nivel.

Facilidad administrativa

Al tener las funciones separadas por capas, administrar la red resulta sencillo.

6.3.3. Principios de diseño de redes jerárquicas

Diámetro de la red

Nos referimos al diámetro de la red como el número de dispositivos que debe de atravesar un paquete desde que se envía hasta que llega al destino deseado. En este diámetro no se tienen en cuenta ni el origen ni el destino. Si queremos reducir los tiempos de latencia, es recomendable que el diámetro se mantenga lo más bajo posible.

Por ejemplo, en la red mostrada anteriormente, si queremos enviar un paquete desde *Laptop0* hasta *IP Phone0*, el diámetro de la red será 3, los tres *switches* que atraviesa, como podemos ver en la siguiente imagen:

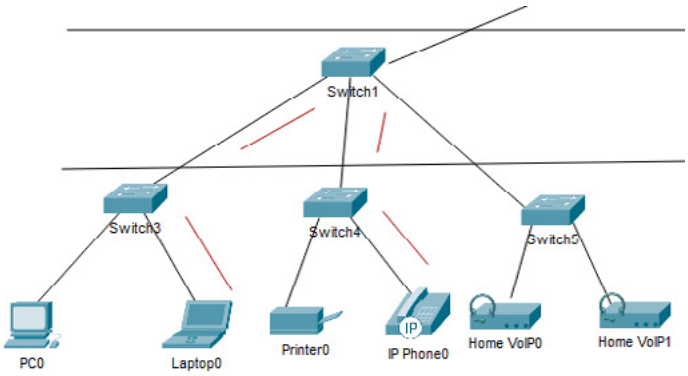

Imagen 22. Diámetro de red 3

Agregación de enlaces

La agregación de enlaces se encuentra regulada por el estándar IEEE 802.1ax y nos permite juntar varios enlaces físicos entre dos dispositivos con la intención de multiplicar en su máximo posible el ancho de banda.

Lo normal es que estos enlaces se creen entre la capa de acceso y la capa de distribución con la intención de que la capacidad de un enlace de gran tráfico sea el que multiplique su capacidad.

Además del ancho de banda, la velocidad de cada puerto con otro también e suman, para conseguir un enlace de alta velocidad. Si hacemos los cálculos necesarios, teniendo en cuenta que se pueden agregar un máximo de 8 puertos, se podría conseguir un máximo de 80Gbps en puertos Ethernet.

Se puede usar esta agregación para cualquiera de los enlaces entre cualquiera de los dispositivos de la red. En Cisco, esto se conoce como *EtherChannel*.

Redundancia

Hay casos en los que la empresa requerirá que la fiabilidad en la red sea muy fuerte, por lo que necesitaremos incorporar cierta redundancia. Para esto, casi siempre recurrimos a lo mismo, duplicar ciertas conexiones entre las capas de distribución y núcleo por si falla alguna, que los *switches* tengan caminos alternativos. Pero hay veces en las que la empresa no necesita redundancia ninguna, al nivel en el que incluso no existe capa de distribución.

En la siguiente imagen podemos ver una red con enlaces duplicados para conseguir la redundancia en la capa de núcleo.

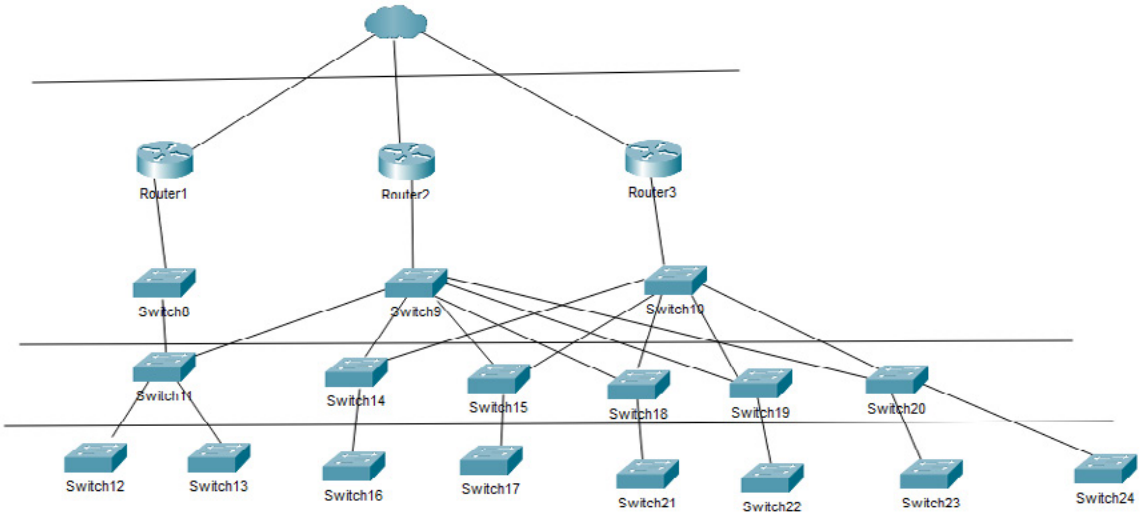

Imagen 23. Red convergente

Red convergente o de nueva generación (NGN)

Nos referimos a las redes convergentes como las que permiten comunicar voz y vídeo con una red de datos, cosa antiguamente imposible para casi todas las empresas. Esta convergencia que se obtiene gracias a las redes modernas, ya que antes eran muy costosas y tediosas en temas de administración. Con las redes convergentes tenemos una mejor y más sencilla administración con una única instalación del cableado.

www.universae.com