switch

Configuración General de un SWITCH

Las siguientes configuraciones son muy generales, todo dependerá de nuestra red y de como está configurada

- Configurar el switch principal (root bridge) con el ID más bajo
- Root port→ Es el puerto con el menor coste para llegar al root bridge
- Designate port→ El es puerto que puede ser designado como root port en caso de caida del root port
- Debemos habilitar el RSTP o el MSTP si tenemos varias VLAN.
- Habilitar el fastlink en los puertos que no sean de enlace con otros switch o dispositivos de capa 2, es decir sólo para dispositivos finales (edge devices→ordenadores, impresoras, etc
- Uplinkfast Si tenemos enlaces redundantes con otro switch, uplinkfast acelera la trasición entre el enlace primario que cae y el secundario que toma el control. Es decir no hay que esperar los 50 s de convergencia de STP.
- deshabilitar el flow control savo que tengamos conectado al swtich un equipo muy viejo
- Habilitarlo el flow control en caso de utilizar jumbo frames

Spanning Tree

- http://www.the-evangelist.info/2010/04/ccnp-switch-8-configuracion-de-spanning-tree/
- http://www.the-evangelist.info/2010/04/ccnp-switch-9-protegiendo-la-topologia-de-spanning-tree/
- http://www.the-evangelist.info/2010/04/ccnp-switch-10-protocolo-spanning-tree-avanzado/
- http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html
- http://capa3.es/bpduguard-y-stp-como-contramedida-a-un-loop-en-un-switch.html

PortFast

Configura un puerto para pasar directamente al estado de direccionamiento **Forwarding** sin esperar por la etapa de escucha y aprendizaje. Para evitar loops portfast no se permite en puertos en modo trunk y lo mejor para evitar problemas es habilitarlo sólo en bocas conectadas a equipos finales (servidores,estaciones, impresoras, etc)

EdgePort

EdgePort es para RSTP lo mismo que PortFast para STP, se configura un puerto como tal cuando se sabe que dicha boca nunca será conectada hacia otro switch y por tanto pasara inmediatamente al estado de direccionamiento sin esperar por las etapas de escucha o aprendizaje que consumen tiempo.

bpduguard

Evita que se reciban tramas BDPU por un puerto . Si lo activamos y se reciben tramas BDPU por dicho puerto lo deshabilita y hay que volver a activar dicha boca manualmente. Lo ideal es activarlo en todas las bocas de los switchs conectados a equipos finales, pero para evitar ataques ponerle un tiempo para que se levante automáticamente dicho puerto una vez pasado un determinado tiempo.

```
Switch(config)# errdisable recovery cause bpduguard
Switch(config)# errdisable recovery interval 30
```

bdpufilter

no permite enviar tramas BPDUs por este puerto. Activar en todas las bocas del los switch de acceso donde se conectan los equipos de los usuarios.

guard root

guard root es similar a bpduguard, pero solo bloquea el puerto si se reciben tramas BPDU indicando la presencia de un equipo más prioritario, el cual sería una nueva raíz del árbol.

En el switch que sea **Root Bridge** hay que activarlo en las bocas que conectan con otros switchs

IGMP

IGMP snooping consiste en escuchar el tráfico IGMP (Internet Group Management Protocol), de forma que el switch crea un mapa de los links que necesitan transmisiones multicast y de esta forma, manejar el tráfico de manera que sólo los puertos que necesitan ese tráfico específico lo reciban.

Referencias

http://www.cisco.com/en/US/docs/switches/lan/catalyst4000/7.4/configuration/guide/stp_enha.html