STP-RSTP y ETHERCHANNEL

Identificación del Problema de Tráfico a Nivel de Capa 2

Las redes conmutadas, funcionan enviando tramas basados en la dirección MAC destino. Este es el comportamiento natural de los conmutadores y es este comportamiento natural, el origen del uso de un Protocolo que evite Loop de Conmutación cuando existe redundancia en la red.

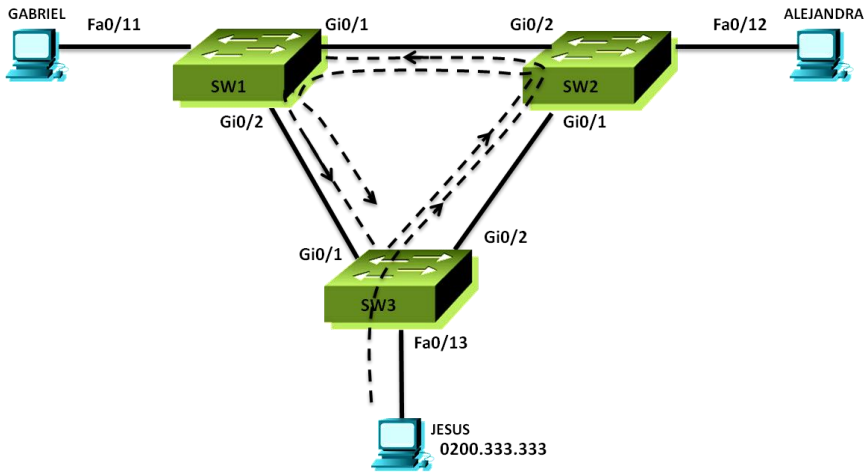
Cuando un computador "X" quiere comunicarse con un Computador "Y", este llega a una interfaz del Switch "A", el cual graba la MAC "X" en la Tabla MAC y la asocia a la interfaz de entrada. Recordemos que los Switches solo relacionan y guardan las direcciones MAC que ingresan por sus interfaces. Seguidamente, si el switch no tiene la dirección "Y" en su tabla de direcciones MAC, inunda la red con un Broadcast de Capa 2, esperando que al computador destino, responda a este llamado. Cuando el computador "Y" responde, envía una trama de regreso y en este momento el Switch, graba la MAC "Y" en su Tabla MAC y la relaciona con la interfaz que recibido la trama. Hasta aquí todo bien.

Sin embargo, cuando existen una red que tiene Redundancia Física, es decir, redundancia en sus enlaces, este comportamiento natural de los Switches, trae consigo otro comportamiento, el de los LOOPS de SWITCHING. Justamente, en el envío o inundación que realiza el Switch en la búsqueda de la MAC destino, también, serpa desconocida por los otros switches de la red, quienes, tampoco conocen donde se encuentra la MAC destino. Esto puede permitir que el Switch que envió la solicitud o inundo la red, vuelva a recibir el paquete por una de sus interfaces, asumiendo que otro switch está solicitando la misma dirección que el solicito o peor aún, alterando los registros de la tabla MAC que ya se encontraban en el.

Este comportamiento, genera los siguientes tres problemas en la red.

1. Exceso o Tormentas de Broadcast
2. Alteración de la Tabla de Direcciones MAC en el SWITCH
3. Exceso de Tráfico en los PC, lo cual genera un incremento en el uso del CPU y la Memoria.

Para sobreponerse a este comportamiento natural de los switches, se requiere de un Protocolo que DETENGA este comportamiento y permita crear una RUTA LIBRE entre un host y otro dentro de un segmento o red conmutada con redundancia y a este mecanismo se le llamo Spanning TREE PROTOCOL.



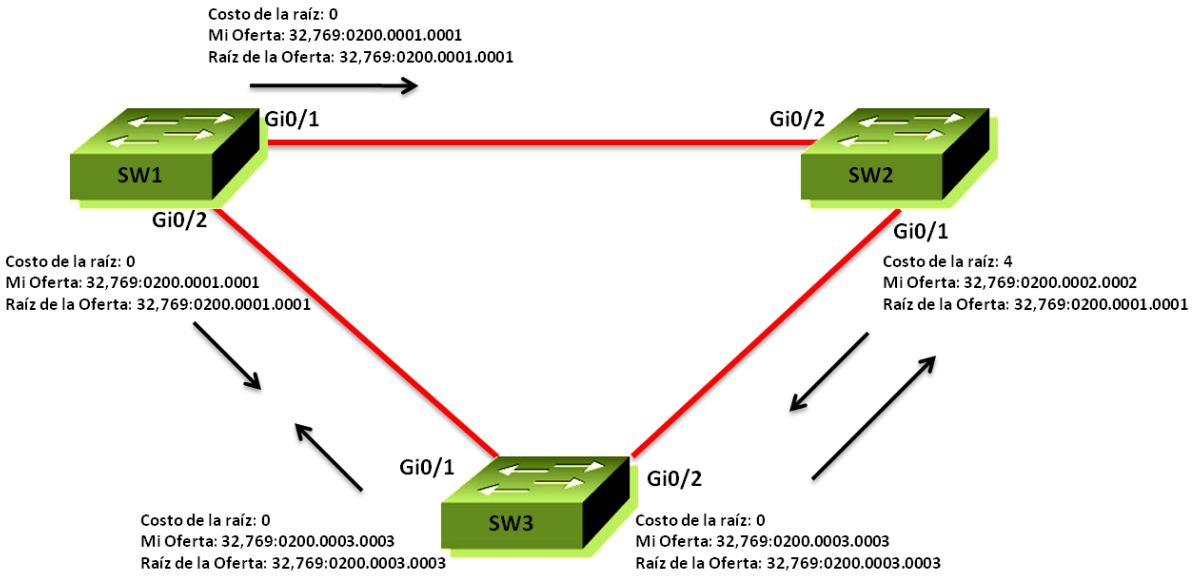
Definición de Spanning Tree Protocol

Spanning Tree Protocol es un Mecanismo o Tecnología de Capa 2 que permite crea una ruta libre de LOOP en una red conmutada con redundancia física.

También conocido como STP, fue definido por el IEEE bajo el estándar IEEE 802.1d.
STP se basa en CST o Common Spanning Tree, el cual, crea una sola instancia de Árbol Jerárquico para todas las VLAN que se crean y administran en el switch.

En los switches Cisco, manejamos PVST+. El cual es un protocolo propietario de Cisco que nos permite, crear una Instancia de Arbol Jerárquico por cada VLAN que creamos y administramos en el Switch. En el mismo orden de ideas, por ser STP un Protocolo, efectivo, pero lento en su convergencia, Cisco ha propuesto una serie de mejoras PROPIETARIAS al STP original, que se orientan a optimizar y mejorar los tiempos de convergencia de la red a nivel de capa 2.

Entre estas mejoras, propuestas por Cisco tenemos: Portfast, UplinkFast, Backbonefast, BPDU Guard, Root Guard, por mencionar las principales.
Pasemos a ver, como trabaja STP y como se forma el árbol STP



Como trabaja STP

STP o IEEE 802.1d, trabaja colocando puertos en ESTADO de ENVIO (FORWARDING) y puertos en ESTADO de BLOQUEO (BLOCKING) para poder lograr una sola RUTA LIBRE DE LOOP.

Para cumplir su tarea, STP, sigue los siguientes pasos:

Elección de un ROOT BRIDGE: Basado en el envío de **BPDU** o BRIDGE PACKET DATA UNIT. Este paquete tiene la responsabilidad de transportar los **Atributos** (valores) que permiten a STP seleccionar el **ROOT BRIDGE** de la red. Esta elección se basa en el menor valor de **PRIORIDAD**, la cuál por defecto es **32768** más el valor del **System ID**, que es igual al valor de la **VLAN**. Por ejemplo, si es la **VLAN 1**, entonces tenemos una **PRIORIDAD igual a 32769 (32768 + 1)**. Si todos los switches tienen el mismo valor de **PRIORIDAD**, entonces el mecanismo de desempate es el **menor valor de Dirección MAC**. Es decir, el **BPDU** de menor valor, es seleccionado el **ROOT BRIDGE** de la red. Seguidamente, todos los puertos del Switch entran en Role **DESIGNADO** y en estado **FORWARDING**. Igualmente, todos los puertos del ROOT BRIDGE, se publican con un **Costo igual a 0** (Cero).

Elección de los ROOT PORT: Los **ROOT PORT**, se eligen en los BRIDGE NO RAIZ. Todos los otros switches distintos al ROOT BRIDGE, son considerados NON ROOT BRIDGE. Todos los NON ROOT BRIDGE, deben **tener un solo ROOT PORT**, el cual siempre estará en ESTADO de ENVIO. **El ROOT PORT es el puerto de menor COSTO hacia el ROOT BRIDGE**. El costo es un valor inverso a la velocidad de la interfaz, siendo la interfaz de mayor velocidad

la de menor **COSTO**. Los Costos de los Enlaces, son definidos por el IEEE. Por ejemplo, un valor de **19** para interfaces **FastEthernet** y un valor de **4** para interfaces **GigaEthernet**.

Elección de los DESIGNATED PORT: Cada Segmento de la red, debe tener un solo Puerto Designado, el cual estará siempre en **ESTADO FORWARDING**. La elección del **DESIGNATED PORT** se basa en el **menor costo del Switch para llegar al ROOT PORT**. Es decir, el costo identificado a través de la interfaz previamente seleccionada como ROOT PORT. Ese costo, es enviado al otro switch del segmento donde se debe seleccionar el DESIGNATED PORT. En caso que un Switch, identifique que tiene el menor costo hacia el ROOT BRIDGE en comparación con los otros switches que participan en la elección del DESIGNATED PORT, el Switch se adjudicará el DESIGNATED PORT de ese segmento. Sin embargo, si los switches identifican que todos tienen el mismo costo para llegar al ROOT BRIDGE a través de sus ROOT PORTS, entonces deben desempatar enviándose su propio **BRIDGE ID (PRIORIDAD+SYSTEM ID+MAC)**. El switch con el menor valor de **BID**, seleccionará su interfaz como **DESIGNATED PORT** y todas las otras interfaces de los otros switches, quedarán en estado de BLOQUEO para así cerrar con la elección de los puertos y cerrar el árbol STP para esa VLAN en específico.

Elección de los Puertos Bloqueados: Los Puertos Bloqueados son aquellos, seleccionados por el STP, para romper el BUCLE que causaría el LOOP de Conmutación. Los Puertos en estado de Bloqueo, tendrán el **"mayor"** costo hacia el ROOT BRIDGE o entre los Puertos Designados.

STP, tiene los siguientes Roles de puertos:

ROOT PORT: El Puerto Raíz, se encuentra siempre en los Switches No Raiz. Es el puerto con el menor costo de ruta hacia el ROOT BRIDGE. Solo existe un ROOT PORT por Switch No Raíz. Se encuentre siempre en estado de envío

DESIGNATED PORT: Es un rol de puerto, que se encuentra siempre en estado de ENVIO. Todos los puertos del ROOT BRIDGE, siempre estarán en estado de envío. En el mismo orden de ideas, todos los segmentos de la red, deben tener un Puerto Designado, el cual es elegido como el puerto de mejor costo hacia el ROOT BRIDGE desde la perspectiva de ese segmento.

STP, define 5 estados de puertos y cada uno de ellos, tiene un funcionamiento dentro de la red. Los Estados de Puertos son los siguientes:

DISABLE: Este es el estado shutdown. Es cuando un puerto esta administrativamente apagado. En este estado el puerto no envía ni recibe tramas.
BLOCKING: Este estado, el puerto no envía ni recibe tramas, ni aprende direcciones MAC. Solo recibe y escucha BPDU.
LISTENING: En este estado, STP permite, aprender BPDU. No envía ni recibe direcciones MAC, tampoco, envía ni recibe tramas.

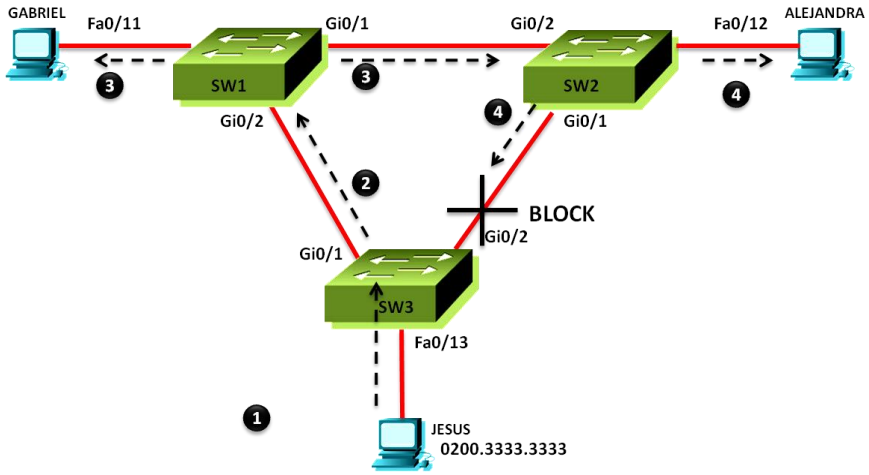
LEARNING: En este estado, se envían y reciben BPDU, así como se aprenden direcciones MAC. No se envían ni se reciben tramas.
FORWARDING: Este es el estado de ENVIO. Un puerto en este estado tiene la capacidad de enviar y recibir BPDU, enviar y aprender Direcciones MAC así como enviar y recibir tramas de capa 2.

De todos los estados, los únicos 2 que son TRANSITORIOS, son LISTENING y LEARNING. Los otros 3 estados DISABLE, FORWARDING y BLOCKING son estados de puertos ESTABLES.

Igualmente, STP, establece 3 tipos de TEMPORIZADORES, los cuales se definen a continuación:

HELLO TIMER: Es igual a 2 segundos. Determina cada cuanto tiempo es enviado un BPDU.
MAX AGE TIMER: Es 20 veces el HELLO TIMER. 20 segundos es el tiempo de espera, que tiene un Switch si no recibe BPDU o un mejor BPDU en STP. Este es el tiempo, que un puerto permanece en estado de BLOQUEO, después de un cambio en la tipología de la red.
FORWARD DELAY: Es igual a 15 segundos. Cuando existe un cambio en la topología de la red, un puerto se mantiene 15 segundos en el estado LISTENNG y 15 segundos más en el estado LEARNING.

En total un cambio en la topología STP, haría que un puerto se mantenga 20 segundos en estado de BLOQUEO, más 15 segundos en estado LISTENING más 15 segundos en estado LEARNING, lo cual sería un total de 50 segundos de espera. Esto es mucho tiempo para que una red conmutada permita el tráfico dentro de la red. En este sentido, Cisco, desarrollo una serie de mejoras para permitir una CONVERGENCIA más rápida en la red conmutada que utilice STP como su mecanismo de protección de loops de capa 2. Estas mejoras las veremos en la próxima sección.



Opciones de mejoras para STP

PORFAST:

- Es una de las mejoras ofrecidas por Cisco.
- Está orientada a la conectividad entre el Switch y equipos finales, como los son, los pc, las laptops, los servidores, las impresoras de red, los puntos de acceso inalámbrico, entre otros.
- PORFAST permite, que un puerto pase del Estado DISABLE al Estado FORWARDING, sin tener que pasar por los estados LISTENING o LEARNING.
- PORTFAST, se habilita a nivel de interfaz y también puede habilitarse, globalmente para todas las interfaces del switch. Es un mecanismo, que se utiliza en los switches de ACCESO.

BPDU GUARD:

- Mecanismo propietario de Cisco.
- Es un mecanismo que protege al SWITCH de recibir mejores BPDU por una interfaz que no debería recibir ningún BPDU.
- Se habilita, normalmente, en interfaces con PORFAST.
- Si una interfaz, con BPDU GUARD habilitado, detecta la recepción de un BPDU, automáticamente desactiva el puerto y lo coloca en err-disable.
- Está desactivado por defecto, aunque se puede activar tanto en la interfaz como globalmente.

BPDU FILTER:

- Mecanismo propietario de Cisco.
- Es un mecanismo que protege al SWITCH de enviar y de recibir mejores BPDU por una interfaz que no debería recibir ningún BPDU.
- Se habilita, normalmente, en interfaces con PORFAST.
- Cuando se activa por interfaz, el switch va a ignorar todas las BPDU que recibe y además, no enviará BPDU por esa interfaz.

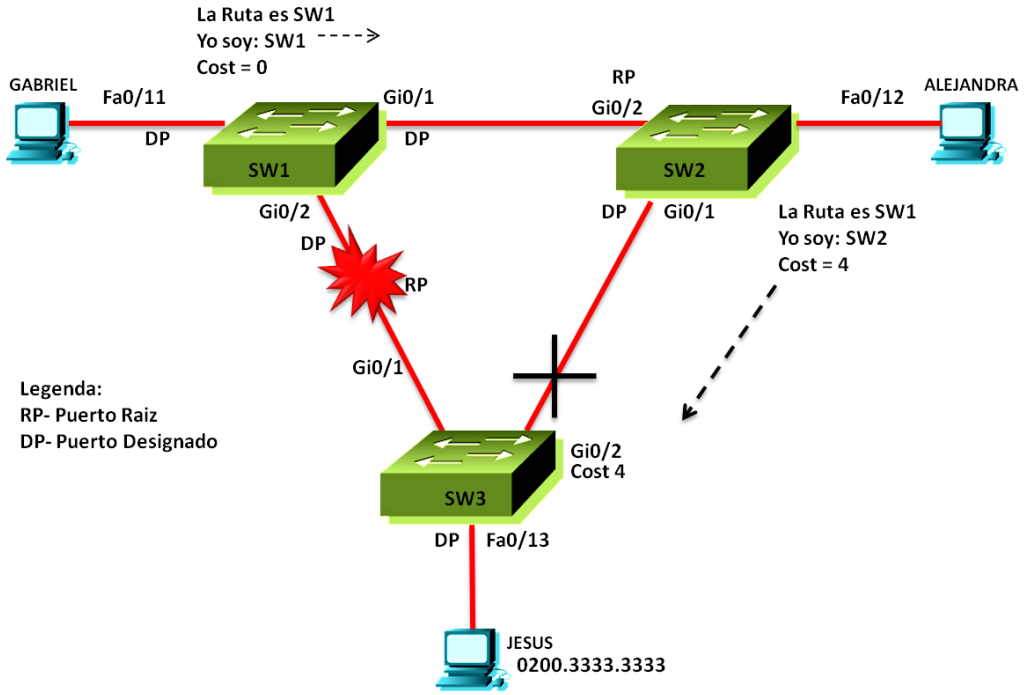
ROOT GUARD:

- Mecanismo propietario de Cisco y se activa por interfaz.
- Permite a un ROOT BRIDGE, detectar y detener cualquier intento de alterar al árbol STP, ya creado.
- Al recibir un BPDU se desactivará el puerto, colocándolo en root-inconsistent.
- Si recibe un mejor BPDU, colocará el puerto en err-disable.
- Una vez, se deje de transmitir este nuevo y mejor BPDU, el switch activa el puerto nuevamente.

LOOP GUARD:

- Mecanismo propietario de Cisco y se activa por interfaz.
- Mantiene una topología libre de loops aun cuando no se reciban BPDU.
- Al recibir un BPDU se desactivará el puerto, colocándolo en loop-inconsistent.

- Debe activarse en interfaces con roles de ROOT PORT y ALTERNATED PORT.
- Se activa tanto por interfaz como globalmente.
- Está desactivado por defecto.



Definición de RSTP

RSTP o Rapid Spanning Tree Protocol, es la mejora del estándar IEEE 802.1d.
RSTP, también es un estándar y está definido bajo el IEEE 802.1w.
Fue diseñado como una mejora de 802.1d permitiendo una más rápida convergencia al existir cambios en la topología de la red.
Es compatible con 802.1d e integra varias funciones propietarias de Cisco, como lo son **Porfast** y **Uplinkfast**.

RSTP, define 3 nuevos roles de puertos, que son:

ALTERNATE: Este rol de puerto, se encuentra siempre en estado de **DISCARDING**. Es el segundo a bordo para convertirse en el **ROOT PORT**. Con el puerto ALTERNATE, el switch no tiene que esperar por los tiempos de convergencia. Si el ROOT PORT falla, el Switch asigna al **ALTERNATE PORT**, el rol de **ROOT PORT** de forma automática.

BACKUP: Este rol de puerto, se encuentra siempre en estado **DISCARDING**. Es el segundo a bordo para convertirse en el **DESIGNATED PORT**. Con el puerto BACKUP, el

switch no tiene que esperar por los tiempos de convergencia. Si el DESIGNATED PORT falla, el Switch asigna al BACKUP PORT, el rol de DESIGNATED PORT de forma automática.
DISABLE: Este puerto se encuentra siempre en modo shutdown.

RSTP, define solo 3 estados de puertos, resumiendo en un solo estado, 3 estados de STP. Los estados de puertos de RSTP, son los siguientes:

1. **DISCARDING**: Este puerto resume los estados DISABLE, LISTENING y BLOCKING.
2. **LEARNING**: Igual que en STP.
3. **FORWARDING**: Igual que en STP.

Los TEMPORIZADORES de RSTP, son los siguientes:

1. **HELLO TIMER:** Es igual a 2 segundos. Determina cada cuanto tiempo es enviado un BPDU.
2. **MAX AGE TIMER:** Es 3 veces el HELLO TIMER. 6 segundos es el tiempo de espera, que tiene un Switch si no recibe BPDU o un mejor BPDU en RSTP. Este es el tiempo, que un puerto permanece en estado de DISCARDING, después de un cambio en la tipología de la red, ya que en el estado LEARNIN, RSTP, se mantiene por muy corto tiempo.
3. **FORWARD DELAY**: En RSTP no se define este Temporizador.

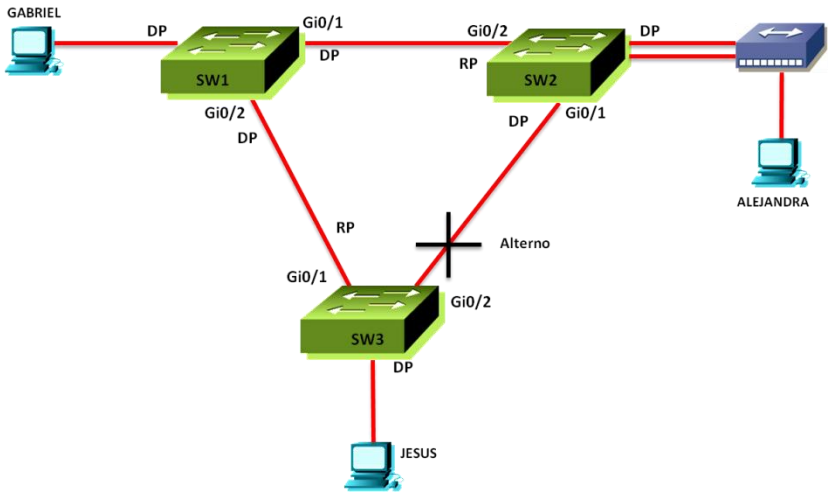
En total un cambio en la topología RSTP, haría que un puerto se mantenga solo 6 segundos en estado de DISCARDING. En este sentido, el tiempo de **CONVERGENCIA** en una red con RSTP, puede ser de 10 segundos, o en muchos casos tan solo de 1 o 2 segundos.

RSTP, reconoce los enlaces físicos dentro de la red y a estos les ha asignado un nombre y una función dentro de la topología de protección de loops de switching. Los enlaces, se definen de la siguiente manera:

EDGE LINK TYPE: Son los enlaces físicos, que conectan los computadores o equipos finales de la red con el switch. Funcionan igual que con Porfast.

POINT TO POINT LINK TYPE: Son los enlaces FULL-DUPLEX. Representa los enlaces entre los switches de la red. RSTP se ejecuta eficientemente en este tipo de enlaces.

SHARED LINK TYPE: Normalmente, en puerto o interfaces que se conectan a una DOMINIO de DOLISION vía un Concentrador o Dispositivo de Capa 1. Son conexiones HALF-DUPLEX. En estos escenarios, RSTP trabaja como STP.



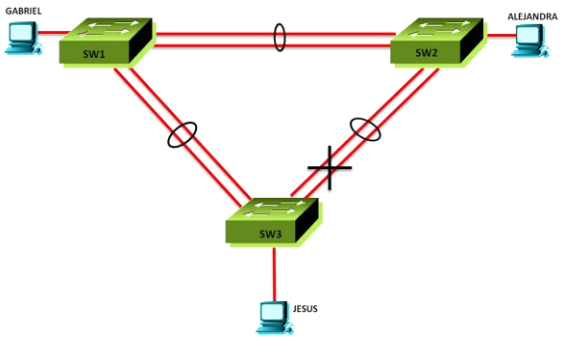
[Definición de Etherchannel de Capa 2]

También conocido como Agregación de Puertos, es una tecnología que permite incrementar el ancho de banda, realizar balanceo de carga y ofrecer en la red, redundancia, física y lógica. Permite establecer un solo canal o interfaz de comunicación lógica entre los switches que forman el etherchannel.

Esta tecnología permite agrupar hasta 8 puertos para crear una sola conexión lógica. Si un cable físico o un puerto del enlace se cae o deja de funcionar, el etherchannel seguirá funcionando con los otros puertos activos que forman la interfaz lógica.

Etherchannel, puede crearse con Protocolo Propietario de Cisco, conocido como Port Aggregation Protocol o PagP, con Protocol Estándar conocido como Link Aggregation Protocol o LacP o de forma manual sin Protocolo definido.

Entre las características de la tecnología etherchannel de cara al CCNA, esta la capacidad de romper con el bucle o redundancia de la red, permitiendo que los puertos bloqueados por el STP pasen al estado de envío, al ser agregados todos como una sola interfaz.



Principales Comandos de STP, RSTP y Etherchannel

COMANDO	DESCRIPCION
SW(config)# spanning-tree mode [pvst | rapid-pvst | mst]	Permite asignar el modo STP, RSTP o MST.
SW(config)# spanning-tree vlan [#vlan] priority [priority]	Permite asignar manualmente la prioridad a un switch de la red en incrementos de 4096.
SW(config)# spanning-tree vlan [#vlan] root [primary | secondary]	Permite definir el manual y explícitamente el Switch Raiz y el Switch secundario en la red. Si se escoge Primary, la prioridad será de 25.576 + VLAN ID. Si se escoge secondary, la prioridad será 28.672 + VLAN ID.
SW(config-if)# spanning-tree vlan [#vlan] cost [cost]	Asigna un costo a la interfaz.
SW(config-if)# spanning-tree vlan [#vlan] priority [priority]	Asigna una prioridad a la interfaz..
Sw(config)# show spanning-tree	Muestra todas las intancias de STP por cada VLAN.
Sw(config)# show spanning-tree vlan [#vlan]	Muestra todas la intancia de STP para una sola VLAN.
Sw(config)# show spanning-tree root	Muestra la información del Switch Raiz para cada VLAN
SW(config-if)# spanning-tree portfast	Habilita portfast en la interfaz.
SW(config)# spanning-tree portfast defautl	Habilita portfast a nivel global.
SW(config-if)# spanning-tree bpduguard enable	Habilita BPDU GUARD en la interfaz.
SW(config-if)# spanning-tree guard root	Habilita ROOT GUARD en la interfaz.
SW(config-if)# channel-protocol [pagp | lacp]	Habilita los protocolos PagP o LacP en la interfaz.
SW(config-if)# channel-group [#grupo] mode [on | auto | desirable | active | passive]	Crea el interfaz lógicA y define el modo de trabajo del etherchannel.
Sw(config)# show etherchannel summary	Muestra la información del etherchannel y sus interfaces.
Sw# debug spanning-tree events	Comando que permite verificar cambios de estados de puertos, asi como los roles de puertos.

The House of Routing
https://cursos.thehouseofrouting.com