RESUMEN – TRABAJO DE GRADO

AUTORES	JORGE EMILIO CLARO
FACULTAD	INGENIERIAS
PLAN DE ESTUDIOS	INGENIERIA DE SISTEMAS
DIRECTOR	FABIAN RANULFO CUESTA QUINTERO Esp. Práctica Docencia Universitaria
TÍTULO DE LA TESIS	PROTOCOLOS DE ÁRBOL DE EXPANSIÓN COMO PLAN DE CONTINGENCIA A LAS REDES REDUNDANTES

RESUMEN
(70 palabras aproximadamente)

LA MONOGRAFÍA PLANTEADA PERMITIÓ REALIZAR UN ANÁLISIS DE LOS DISTINTOS PROTOCOLOS QUE SE ENCARGAN DE COMUNICAR LOS SWITCHS DE LA RED, EVITANDO LA FORMACIÓN DE BUCLES Y CONTROLANDO EL EXCESO DE TIEMPO TOMADO TANTO EN LA CREACIÓN DEL ÁRBOL DE EXPANSIÓN COMO DE RECONFIGURACIÓN EN CASO DE QUE SE PRODUJERA LA CAÍDA DE UN ENLACE O EL BLOQUEO, ESTA PROPUESTA ES DE TIPO ANÁLISIS DE EXPERIENCIAS YA QUE SE REALIZA A PARTIR DE LOS CONOCIMIENTOS ADQUIRIDOS.

CARACTERÍSTICAS

PÁGINAS:	PLANOS:	ILUSTRACIONES:	CD-ROM: 1

PROTOCOLOS DE ÁRBOL DE EXPANSIÓN COMO PLAN DE CONTINGENCIA A LAS REDES REDUNDANTES

AUTOR

JORGE EMILIO CLARO

Trabajo de grado presentado bajo la modalidad de monografía para obtener el título de Ingeniero de Sistemas

Director

FABIAN RANULFO CUESTA QUINTERO

Esp. Práctica Docencia Universitaria

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERÍAS

INGENIERÍA DE SISTEMAS

Ocaña, Colombia Mayo, 2018

Agradecimientos

A Dios por darme paciencia y permitirme disfrutar y vivir este triunfo, esta etapa de mi vida que termina para continuar otra donde sé que también estará el conmigo para darme una gran guía para seguir con meta.

Por medio de esta presente monografía damos a conocer nuestros sinceros agradecimientos primeramente a mi madre JULIA BAYONA, quien me ha brindado todo su apoyo incondicional.

También al Ing. Fabián Cuesta quien con paciencia y conocimientos me ha sabido guiar en el transcurso del presente trabajo investigativo y de esta manera culminar el mismo.

.

Dedicatoria

Para realizar esta monografía he recurrido a personas que me han ayudado con tiempo, ideas, sugerencias que al final se ven plasmados en mi trabajo.

A mi madre y a mis hermanos que me dan su apoyo en cada uno de los pasos que doy en todo momento para culminar con éxito este trabajo.

Quienes aportaron para el desarrollo de mi monografía trabaje voluntariamente con amor y desinterés, hago todo con las mejores intenciones, por ser ellos apoyo constantemente en la realización de mis metas y proyectos.

Índice

Lista de Figuras

Lista de Tablas

Introducción

La rápida evolución a la que están sometidas las nuevas tecnologías en el mundo de las telecomunicaciones, provoca que en periodos cortos de tiempo, las grandes o pequeñas empresas e incluso los particulares se vean obligados a renovar las tecnologías o programas que hasta ese momento utilizaban, para poder sacar el máximo provecho a los servicios que ofrecen los mismos (Ingenieros 2007). Los protocolos que se analizaron en esta monografía son: el STP, que significa Spanning Tree Protocol, el RSTP o Rapid Spanning Tree Protocol y el MSTP o Múltiple Spanning Tree Protocol. El fundamento principal de estos protocolos es la creación, en una red compuesta por switch, de un árbol de expansión evitando de esta forma la creación de bucles y permitiendo la reconfiguración del árbol si se presenta algún un fallo en un enlace o en un puente. La redundancia, sin embargo, crea bucles en los que un paquete o varias copias de un paquete pueden ir de un puente a otro de forma indefinida.

Resumen

La monografía planteada permitió realizar un análisis de los distintos protocolos que se encargan de comunicar los switchs de la red, evitando la formación de bucles y controlando el exceso de tiempo tomado tanto en la creación del árbol de expansión como de reconfiguración en caso de que se produjera la caída de un enlace o el bloqueo de un switch. El tipo de monografía planteada en esta propuesta es de tipo análisis de experiencias ya que se realiza a partir de los conocimientos adquiridos en el curso de profundización entornos LAN y WAN ofrecidos por la Universidad Francisco de Paula Santander de Ocaña.

Capítulo 1. Redundancia de LAN

La redundancia de red es clave para mantener la confiabilidad de la red. Varios enlaces físicos entre dispositivos proporcionan rutas redundantes. De esta forma, la red puede continuar funcionando si falló un único enlace o puerto. Los enlaces redundantes también pueden compartir la carga de tráfico y aumentar la capacidad. Se deben administrar varias rutas para que no se produzcan bucles en la capa 2. Se eligen las mejores rutas, y se cuenta con una ruta alternativa de inmediato en caso de que falle una ruta principal. Los protocolos de árbol de expansión se utilizan para administrar la redundancia de capa 2. Los dispositivos redundantes, como los routers o los switches multicapa, proporcionan la capacidad de que un cliente utilice un gateway predeterminado alternativo en caso de que falle el gateway predeterminado principal. Es posible que ahora un cliente posea varias rutas a más de un gateway predeterminado posible. Los protocolos de redundancia de primer salto se utilizan para administrar la forma en que se asigna un gateway predeterminado a un cliente y permitir el uso de un gateway predeterminado alternativo en caso de que falle el principal (Ibanez 2005).

1.1 Redundancia en la capa 1 Y 2 del modelo OSI

La redundancia en la capa 1 del modelo OSI se representa mediante el uso de varios enlaces y dispositivos, pero se necesita más que solo la planificación física para completar la configuración de la red. Para que la redundancia funcione de forma sistemática, también se deben utilizar protocolos de capa 2 del modelo OSI, como STP (CISCO 2013). La redundancia es una parte importante del diseño jerárquico para evitar que se interrumpa la entrega de los

servicios de red a los usuarios. Las redes redundantes requieren la adición de rutas físicas, pero la redundancia lógica también debe formar parte del diseño. Sin embargo, las rutas redundantes en una red Ethernet conmutada pueden causar bucles físicos y lógicos en la capa 2. Los bucles físicos en la capa 2 pueden ocurrir como consecuencia del funcionamiento normal de los switches, en especial, del proceso de descubrimiento y reenvío. Cuando existen varias rutas entre dos dispositivos en una red y no se implementan protocolos de árbol de expansión en los switches, ocurre un bucle en la capa 2 (Ingenieros 2007).

Inestabilidad de la base de datos mac. Las tramas de Ethernet no poseen un atributo de tiempo de vida (TTL) como los paquetes IP. Como resultado, si no hay un mecanismo habilitado para bloquear la propagación continua de estas tramas en una red conmutada, continúan propagándose entre los switches incesantemente, o hasta que un enlace se interrumpa y rompa el bucle. Esta propagación continua entre switches puede provocar la inestabilidad de la base de datos MAC. Esto puede ocurrir a causa del reenvío de tramas de difusión. Las tramas de difusión se reenvían por todos los puertos de switch, excepto por el puerto de entrada original. Esto asegura que todos los dispositivos en un dominio de difusión reciban la trama. Si hay más de una ruta para reenviar la trama, se puede formar un bucle infinito. Cuando ocurre un bucle, la tabla de direcciones MAC en un switch puede cambiar constantemente con las actualizaciones de las tramas de difusión, lo que provoca la inestabilidad de la base de datos MAC (Ibanez 2005). Debido a que se reenvían las mismas tramas constantemente entre todos los switches en el bucle, la CPU del switch debe procesar una gran cantidad de datos. Esto disminuye el rendimiento del switch cuando llega tráfico legítimo. Un host atrapado en un bucle de red es inaccesible para otros hosts de la red. Además, debido a los constantes cambios en la tabla de direcciones MAC,

el switch no sabe cuál es el puerto por el que debe reenviar las tramas de unidifusión. Al haber cada vez más tramas que forman bucles en la red, con el tiempo, se crea una tormenta de difusión.

Tormentas de difusión tormenta de difusión. Una tormenta de difusión se produce cuando existen tantas tramas de difusión atrapadas en un bucle de Capa 2, que se consume todo el ancho de banda disponible. Como consecuencia, no hay ancho de banda disponible para el tráfico legítimo y la red deja de estar disponible para la comunicación de datos. Esto es una denegación de servicio eficaz. La tormenta de difusión es inevitable en una red con bucles. A medida que más dispositivos envían difusiones a través de la red, más tráfico se concentra en el bucle, lo que consume recursos (CISCO 2013). Finalmente, se crea una tormenta de difusión que hace fallar la red. Existen otras consecuencias de las tormentas de difusión. Debido a que el tráfico de difusión se envía a todos los puertos del switch, todos los dispositivos conectados deben procesar todo el tráfico de difusión que fluye indefinidamente en la red con bucles. Esto puede hacer que la terminal no funcione bien a causa de los altos requisitos de procesamiento para mantener una carga de tráfico tan elevada en la NIC. A medida que más dispositivos envían difusiones a través de la red, más tráfico se concentra en el bucle, lo que consume recursos. Finalmente, se crea una tormenta de difusión que hace fallar la red. Cuando la red se satura por completo con tráfico de difusión que genera un bucle entre los switches, el switch descarta el tráfico nuevo porque no lo puede procesar. Dado que los dispositivos conectados a una red envían regularmente tramas de difusión, como las solicitudes de ARP, se puede formar una tormenta de difusión en segundos. Como resultado, cuando se crea un bucle, la red conmutada se desactiva con rapidez (Ibanez 2005).

Tramas de unidifusión duplicadas. Las tramas de difusión no son el único tipo de tramas que son afectadas por los bucles. Las tramas de unicast enviadas a una red con bucles pueden generar tramas duplicadas que llegan al dispositivo de destino. La mayoría de los protocolos de capa superior no están diseñados para reconocer las transmisiones duplicadas o lidiar con ellas. En general, los protocolos que utilizan un mecanismo de numeración en secuencia asumen que la transmisión ha fallado y que el número de secuencia se ha reciclado para otra sesión de comunicación(CISCO 2013) . Otros protocolos intentan enviar la transmisión duplicada al protocolo de capa superior adecuado para que sea procesada y posiblemente descartada. Los protocolos LAN de capa 2, como Ethernet, carecen de mecanismos para reconocer y eliminar las tramas que forman bucles incesantes. Algunos protocolos de capa 3 implementan un mecanismo de TTL que limita la cantidad de veces que un dispositivo de red de capa 3 puede volver a transmitir un paquete. Los dispositivos de capa 2, que carecen de este mecanismo, continúan retransmitiendo de forma indefinida el tráfico que genera bucles. STP, un mecanismo que sirve para evitar los bucles en la capa 2, se desarrolló para enfrentar estos problemas. Para evitar que ocurran estos problemas en una red redundante, se debe habilitar algún tipo de árbol de expansión en los switches. De manera predeterminada, el árbol de expansión está habilitado en los switches Cisco para prevenir que ocurran bucles en la capa 2 (Ingenieros 2007).

1.2 Algoritmo de árbol de expansión

1.2.1 Funciones de puerto. La versión IEEE 802.1D de STP utiliza el algoritmo de árbol de expansión (STA) para determinar qué puertos de switch de una red se deben colocar en estado de bloqueo y evitar que ocurran bucles. El STA designa un único switch como puente raíz y lo

utiliza como punto de referencia para todos los cálculos de rutas. El puente raíz se elige mediante un proceso de elección. Todos los switches que comparten STP intercambian tramas de BPDU para determinar el switch que posee el menor ID de puente (BID) en la red. El switch con el menor BID se transforma en el puente raíz en forma automática según los cálculos del STA (Ibanez 2005).

Cada switch posee una dirección MAC única asociada a la VLAN 1. Una BPDU es una trama de mensaje que intercambian los switches para STP. Cada BPDU contiene un BID que identifica al switch que envió la BPDU. El BID contiene un valor de prioridad, la dirección MAC del switch emisor y una ID de sistema extendido optativa. El valor de BID más bajo lo determina la combinación de estos tres campos. Después de determinar el puente raíz, el STA calcula la ruta más corta hacia dicho puente. Todos los switches utilizan el STA para determinar los puertos que deben bloquearse. Mientras el STA determina las mejores rutas al puente raíz para todos los puertos de switch en el dominio de difusión, se evita que el tráfico se reenvíe a través de la red. El STA tiene en cuenta tanto los costos de ruta como de puerto cuando determina qué puertos bloquear. El costo de la ruta se calcula mediante los valores de costo de puerto asociados con las velocidades de los puertos para cada puerto de switch que atraviesa una ruta determinada. La suma de los valores de costo de puerto determina el costo de ruta total para el puente raíz. Si existe más de una ruta a escoger, el STA elige la de menor costo de ruta (Ibanez 2005).

Una vez que el STA determinó las rutas más deseables en relación con cada switch, asigna funciones de puerto a los puertos de switch que participan. Las funciones de puerto describen la relación que estos tienen en la red con el puente raíz y si se les permite reenviar tráfico.

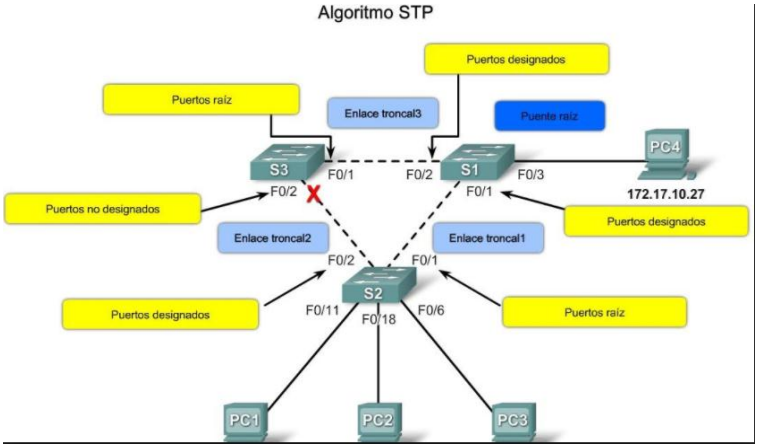

Figura 1. Algoritmo STP
Fuente. (Ingenieros 2007)

Puertos raíz: los puertos de switch más cercanos al puente raíz. Los puertos raíz se seleccionan por switch.

Puertos designados: todos los puertos que no son raíz y que aún pueden enviar tráfico a la red. Los puertos designados se seleccionan por enlace troncal. Si un extremo de un enlace troncal es un puerto raíz, el otro extremo es un puerto designado. Todos los puertos en el puente raíz son puertos designados (CISCO 2013).

Puertos alternativos y de respaldo: Los puertos alternativos y de respaldo están configurados en estado de bloqueo para evitar bucles. Los puertos alternativos se seleccionan solo en los enlaces troncales en los que ninguno de los extremos es un puerto raíz. Esto permite una transición más rápida al estado de reenvío, cuando es necesario. (Los puertos en estado de

bloqueo solo entran en acción cuando hay dos puertos en el mismo switch conectados entre sí mediante un hub o un único cable) (CISCO 2013).

Puertos deshabilitados: un puerto deshabilitado es un puerto de switch que está desactivado.

1.2.2 Puente raíz. Todas las instancias de árbol de expansión (LAN conmutada o dominio de difusión) tienen un switch designado como puente raíz. El puente raíz sirve como punto de referencia para todos los cálculos de árbol de expansión para determinar las rutas redundantes que deben bloquearse. Un proceso de elección determina el switch que se transforma en el puente raíz. En la figura #, se muestran los campos de BID. El BID está compuesto por un valor de prioridad, una ID de sistema extendido y la dirección MAC del switch (CISCO 2013). Todos los switches del dominio de difusión participan del proceso de elección. Una vez que el switch arranca, comienza a enviar tramas BPDU cada dos segundos. Estas BPDU contienen el BID del switch y la ID de raíz. A medida que los switches reenvían sus tramas BPDU, los switches adyacentes en el dominio de difusión leen la información de la ID de raíz de las tramas BPDU. Si la ID de raíz que se recibe de una BPDU es inferior a la ID de raíz del switch receptor, este switch actualiza su ID de raíz e identifica al switch adyacente como puente raíz. En realidad, es posible que no sea un switch adyacente, ya que puede ser cualquier otro switch en el dominio de difusión. Luego el switch envía nuevas tramas de BPDU con el menor ID de raíz a los otros switches adyacentes. Finalmente, el switch con el menor BID es el que se identifica como puente raíz para la instancia de árbol de expansión. Se elige un puente raíz para cada instancia de árbol de expansión (Ibanez 2005). Es posible tener varios puentes raíz diferente. Si todos los puertos

de todos los switches pertenecen a la VLAN 1, solo se da una instancia de árbol de expansión. La ID de sistema extendido cumple una función en la determinación de las instancias de árbol de expansión.

Figura 2. Campos de BID
Fuente. (CISCO 2013)

1.2.3 Costo de la ruta. Una vez que se eligió el puente raíz para la instancia de árbol de expansión, el STA comienza el proceso para determinar las mejores rutas hacia el puente raíz desde todos los destinos en el dominio de difusión. La información de ruta se determina mediante la suma de los costos individuales de los puertos que atraviesa la ruta desde el destino al puente raíz. Cada "destino" es, en realidad, un puerto de switch. Los costos de los puertos predeterminados se definen por la velocidad a la que funcionan los mismos (Ibanez 2005). Como se muestra en la figura 1, el costo de puerto de los puertos Ethernet de 10 Gb/s es 2, el de los puertos Ethernet de 1 Gb/s es 4, el de los puertos Ethernet de 100 Mb/s es 19 y el de los puertos Ethernet de 10 Mb/s es 100. Nota: a medida que se introducen tecnologías Ethernet más modernas y veloces en el mercado, es posible que se modifiquen los valores de costo de ruta para admitir las distintas velocidades disponibles. Los números no lineales de la tabla incluyen algunas mejoras del antiguo estándar Ethernet. Los valores ya se modificaron para admitir el estándar Ethernet de 10 Gb/s. Para ilustrar el cambio continuo relacionado con la tecnología de redes de alta velocidad, los switches Catalyst 4500 y 6500 admiten un método de costo de ruta mayor; por ejemplo, el costo de la ruta de 10 Gb/s es 2000, el de 100 Gb/s es 200 y el de 1 Tb/s

es 20. Pese a que los puertos de switch cuentan con un costo de puerto predeterminado asociado a los mismos, tal costo puede configurarse. La capacidad de configurar costos de puerto individuales le da al administrador la flexibilidad para controlar de forma manual las rutas de árbol de expansión hacia el puente raíz (Stp 2010). El costo de la ruta es igual a la suma de todos los costos de puerto a lo largo de la ruta hacia el puente raíz. Las rutas con el costo más bajo se convierten en las preferidas, y el resto de las rutas redundantes se bloquean.

Tabla 1.
Mejores rutas puente raíz

Velocidad de enlace	Costo (IEEE revisada)	Costo (IEEE anterior)
10 Gb/s	2	1
1 Gb/s	4	1
100 Mb/s	19	10
10 Mb/s	100	100

Fuente. Autor del proyecto

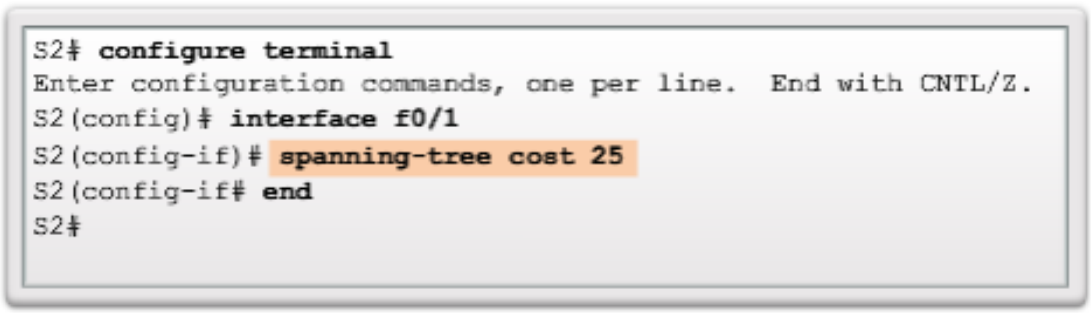

Figura 3. Configuración del costo del puerto
Fuente. Autor del proyecto (Cisco Packet Tracer)

```
S2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)# interface f0/1
S2(config-if)# no spanning-tree cost
S2(config-if)# end
S2#
```

Figura 4. Restablecer costo del puerto
Fuente. Autor del proyecto (Cisco Packet Tracer)

```
S2# show spanning-tree

VLAN001
   Spanning tree enabled protocol ieee
   Root ID     Priority  24577
               Address       000A.0033.3333
               Cost          19
               Port          1
               Hello Time    2 sec Max Age 20 sec Forward Delay 15 sec

   Bridge ID   Priority      32769  (priority 32768 sys-id-ext  1)
               Address 000A.0011.1111
               Hello time 2 sec Max Age 20 sec Forward Delay 15 sec
               Aging Time 300

Interface    Role   Sts  Cost    Prio.Nbr  Type
-----------  -----  ---- -----   --------- ------------------
F0/1         Root   FWD   19       128.1     Edge P2p
F0/2         Desg   FWD   19       128.2     Edge P2p
```

Figura 5. Comando para visualizar las rutas del puente raíz
Fuente. Autor del proyecto (Cisco Packet Tracer)

Capítulo 2. Variedades de protocolos de árbol de expansión

La siguiente tabla muestra los principales protocolos en lo concerniente a protocolos de expansión.

Tabla 2.
Características del protocolo de árbol de expansión

Protocolo	Estándar	Recursos necesarios	Convergencia	Cálculo de árbol
STP	802.1D	Baja	Lento	Todo VLAN
PVST+	Cisco	Alto	Lento	Por VLAN
RSTP	802.1w	Medio	Rápido	Todo VLAN
PVST+rápido	Cisco	Muy alto	Rápido	Por VLAN
MSTP	802.1s, Cisco	Medio o alto	Rápido	Por instancia

Fuente. Autor del proyecto

2.1 PVST+

El estándar IEEE 802.1D original define un árbol de expansión común (CST) que asume solo una instancia de árbol de expansión para toda la red conmutada, independientemente de la cantidad de VLAN. Las redes que ejecutan CST presentan las siguientes características.

- No es posible compartir la carga.
- Un uplink debe bloquear todas las VLAN.

Se preserva la CPU. Solo se debe calcular una instancia de árbol de expansión. Cisco desarrolló PVST+ para que una red pueda ejecutar una instancia independiente de la implementación de Cisco de IEEE 802.1D para cada VLAN en la red. Con PVST+, un puerto de enlace troncal en un switch puede bloquear una VLAN sin bloquear otras. PVST+ se puede

utilizar para implementar el balanceo de carga de capa 2. Debido a que cada VLAN ejecuta una instancia de STP distinta, los switches en un entorno PVST+ requieren un mayor procesamiento de CPU y un mayor consumo de ancho de banda de BPDU que la implementación de CST tradicional de STP. En un entorno PVST+, los parámetros de árbol de expansión se pueden ajustar para que la mitad de las VLAN reenvíen en cada enlace troncal de uplink. El balanceo de carga puede funcionar de forma óptima. Una instancia de árbol de expansión para cada VLAN que se mantiene puede significar un gran desperdicio de ciclos de CPU para todos los switches en la red (además del ancho de banda que se utiliza en cada instancia para enviar su propia BPDU). Esto solo representaría un problema si se configurara una gran cantidad de redes VLAN (Ingenieros 2007).

2.1.1 Estados de los puertos y funcionamiento de PVST+ STP. Facilita la ruta lógica sin bucles en todo el dominio de difusión (Ibanez 2005). El árbol de expansión se determina a través de la información obtenida en el intercambio de tramas de BPDU entre los switches interconectados. Para facilitar el aprendizaje del árbol de expansión lógico, cada puerto de switch sufre una transición a través de cinco estados posibles y tres temporizadores de BPDU. El árbol de expansión queda determinado inmediatamente después de que el switch finaliza el proceso de arranque. Si un puerto de switch pasa directamente del estado de bloqueo al de reenvío sin información acerca de la topología completa durante la transición, el puerto puede crear un bucle de datos temporal. Por este motivo, STP introduce los cinco estados de puerto (Stp 2010).

Tabla 3.
Estados de los puertos

Operación Permitida	Estado del Puerto				
	Bloquear	Escuchar	Aprendizaje	Reenvio	Deshabilitado
Puede recibir y procesar BPDU	Si	Si	Si	Si	No
Puede reenviar tramas de datos recibidas en la interfaz	No	No	No	Si	No
Puede reenviar tramas de datos desde otra interfaz	No	No	No	Si	No
Puede descubrir las direcciones MAC	No	No	Si	Si	No

Fuente. Autor del proyecto

2.2 PVST+ RÁPIDO RSTP (IEEE 802.1w)

Es una evolución del estándar 802.1D original y se incorpora al estándar IEEE 802.1D-2004. La terminología de STP 802.1w sigue siendo fundamentalmente la misma que la de STP IEEE 802.1D original (CISCO 2013). La mayoría de los parámetros no se modificaron, de modo que los usuarios familiarizados con STP pueden configurar el nuevo protocolo con facilidad. PVST+ rápido es, simplemente, la implementación de Cisco de RSTP por VLAN. Con PVST+ rápido, se ejecuta una instancia de RSTP independiente para cada VLAN. RSTP no posee el estado de puerto de bloqueo. RSTP define los estados de puertos como de descarte, aprender o enviar. RSTP aumenta la velocidad de recálculo del árbol de expansión cuando cambia la topología de la red de la Capa 2. RSTP puede lograr una convergencia mucho más rápida en una red configurada en forma adecuada, a veces sólo en unos pocos cientos de milisegundos. RSTP redefine los tipos de puertos y sus estados. Si un puerto está configurado como puerto alternativo o de respaldo, puede cambiar automáticamente al estado de reenvío sin esperar a que converja la red. A continuación se describen brevemente las características de RSTP (Stp 2010):

RSTP es el protocolo preferido para evitar los bucles de Capa 2 en un entorno de red conmutada. La mayoría de las diferencias se establecieron con las mejoras del estándar 802.1D original exclusivas de Cisco. Estas mejoras, como las BPDU que transportan y envían información acerca de las funciones de los puertos sólo a los switches vecinos, no requieren configuración adicional y por lo general poseen un mejor rendimiento que las versiones anteriores propiedad de Cisco. Ahora son transparentes y se integran al funcionamiento del protocolo (Kern et al. 2006).

Las mejoras al estándar 802.1D original exclusivas de Cisco, como UplinkFast y BackboneFast, no son compatibles con RSTP.

RSTP (802.1w) reemplaza al estándar 802.1D original y, al mismo tiempo, mantiene la compatibilidad con versiones anteriores. Se mantiene la mayor parte de la terminología del estándar 802.1D original, y la mayoría de los parámetros no se modificaron. Además, 802.1w se puede revertir al estándar 802.1D antiguo para interoperar con switches antiguos por puerto. Por ejemplo, el algoritmo de árbol de expansión de RSTP elige un puente raíz de la misma forma que lo hace el estándar 802.1D original (Cinkler et al. 2005).

RSTP mantiene el mismo formato de BPDU que el estándar IEEE 802.1D original, excepto que el campo Versión está establecido en 2 para indicar el protocolo RSTP y el campo Indicadores utiliza los 8 bits.

RSTP puede confirmar de manera activa que un puerto puede sufrir una transición segura al estado de enviar sin depender de ninguna configuración de temporizadores.

2.3 Multiple spanning tree protocol (MSTP)

IEEE 802.1s Multiple Spanning Tree Protocol usa el concepto de LAN virtual (VLAN), el cual es una colección de múltiples LANs que se encuentran conectadas físicamente a una red compartida y operan como si todas esas redes múltiples estuvieran conectadas virtualmente como una sola LAN. MSTP permite solamente 4096 VLANs en una red debido a los 12 bits del VLAN ID definidos por IEEE 802.1Q. MSTP introduce el concepto de región y cada región dispone de su propia VLAN asignada. Una región representa un grupo de switches que tienen el mismo identificador de región y la misma VLAN asignada. Cada región dispone de sus instancias MST, multiple spanning tree (CISCO 2013). El rol de las instancias MST es optimizar la utilización de la red, mientras que las regiones MST pueden ser usadas para incrementar la escalabilidad de la red, también pueden ser utilizadas para mejorar el tiempo de reacción en caso de fallo en la red. Las regiones están conectadas directamente con una instancia central del STP. Dentro de una región MST, posiblemente haya varias instancias MST. El protocolo MSTP proporciona un máximo de 64 instancias de árbol de expansión en una región (Cinkler et al. 2005).

El uso de MSTP permite la utilización de todos los enlaces que serían de lo contrario inutilizados por el árbol simple de expansión y de ese modo elimina la pérdida de ancho de ancho de banda. Sin embargo, el árbol de expansión construido en una región sigue esencialmente el protocolo RSTP y eso conlleva, de forma inherente, a que los tiempos de

restauración sean los de RSTP, pero en este caso vinculados con el tamaño de la VLAN en la que nos encontramos. Además, el proceso básico de aprendizaje asocia las direcciones MAC con puertos/enlaces de tal forma que si un enlace falla causaría que los puentes irían a una reasignación de VLAN si el tráfico fuera a ser mapeado hacia un árbol de expansión alternativo (Stp 2010).

Una particularidad que hay que tener en cuenta cuando hablamos de MSTP, es el uso de VLANs, lo que provoca que necesitemos etiquetar de forma distinta los mensajes pertenecientes a una VLAN o a otra, para poder discriminarlos llegado el momento. La necesidad de etiquetar los mensajes hace necesario comunicar los conmutadores de forma que dejen pasar todos los mensajes independientemente de a que VLAN pertenezcan para que la red trabaje de forma unida. Esto es posible si identificamos los enlaces/puertos entre conmutadores como enlaces Trunk, lo que nos permitirá discriminar los paquetes que nos interesen en el conmutador, dejándolos pasar por los puertos que correspondan a la VLAN deseada(Kern et al. 2006).

Capítulo 3. Configuración predeterminada de UN SWITCH CATALYST 2960 PARA PVST+

En la tabla, a continuación, se muestra la configuración predeterminada de árbol de expansión para un switch Cisco de la serie Catalyst 2960.

Característica	Configuración predeterminada
Estado habilitado	Habilitado en la VLAN 1
Modo de árbol de expansión	PVST+ (PVST+ rápido y MSTP están deshabilitados)
Prioridad de switch	32768
Prioridad de puerto de árbol de expansión (configurable por interfaz)	128
Costo de puerto de árbol de expansión (configurable por interfaz)	1000 Mb/s: 4 100 Mb/s: 19 10 Mb/s: 100
Prioridad de puerto de VLAN de árbol de expansión (configurable por VLAN)	128
Costo de puerto de VLAN de árbol de expansión (configurable por VLAN)	1000 Mb/s: 4 100 Mb/s: 19 10 Mb/s: 100
Temporizadores de árbol de expansión	Tiempo de saludo: 2segundos Tiempo de retraso de reenvío: 15 segundos Tiempo máximo de vencimiento: 20 segundos Conteo de espera de transmisión: 6BPDU

Figura 6. Configuración de un switch de manera predeterminada
Fuente. (Anon n.d.), (CISCO 2013)

3.1 Configuración y verificación de la ID de puente

Cuando un administrador desea seleccionar un switch específico como puente raíz, se debe ajustar el valor de prioridad del puente para asegurarse de que sea inferior a los valores de prioridad del puente del resto de los switches en la red. Existen dos métodos diferentes para

configurar el valor de prioridad del puente en un switch Cisco Catalyst (CISCO NETACAD n.d.).

3.1.1 Método 1. Para asegurar que un switch tenga el valor de prioridad de puente más bajo, utilice el comando spanning-tree vlan id-vlan root primary en el modo de configuración global. La prioridad para el switch está establecida en el valor predefinido 24576 o en el múltiplo más alto de 4096, menos que la prioridad del puente más baja detectada en la red. Si se desea otro puente raíz, utilice el comando spanning-tree vlan id-vlan root secondary del modo de configuración global. Este comando establece la prioridad para el switch en el valor predeterminado 28672. Esto asegura que el switch alternativo se convierta en el puente raíz si falla el puente raíz principal. Se supone que el resto de los switches en la red tienen definido el valor de prioridad predeterminado 32768 (Cinkler et al. 2005).

En la figura 7, el S1 se asignó como puente raíz principal mediante el comando spanning-tree vlan 1 root primary, y el S2 se configuró como puente raíz secundario mediante el comando spanning-tree vlan 1 root secondary.

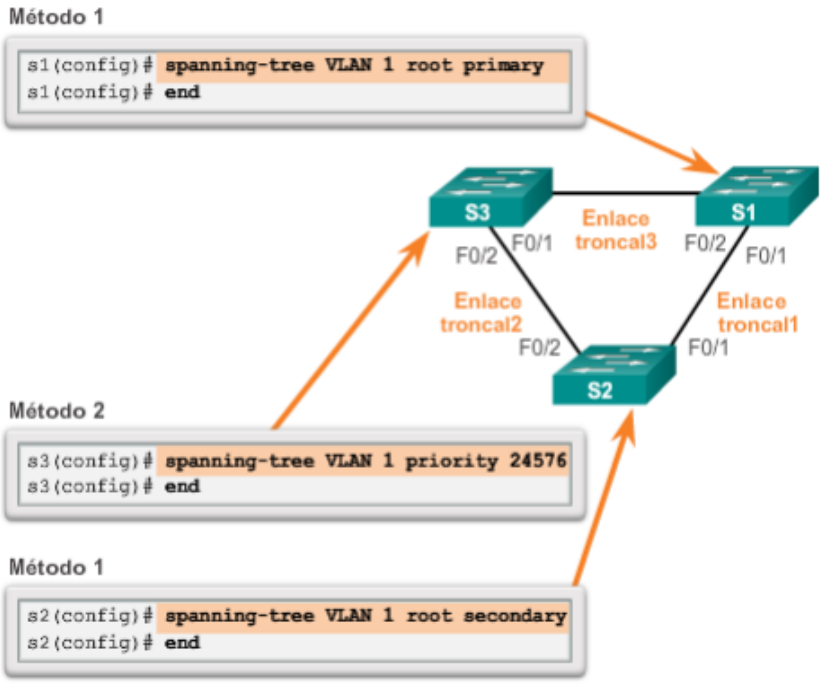

Figura 7.Configurar y verificar el BID
Fuente. (CISCO 2013)

3.1.2 Método 2. Para configurar el valor de prioridad del puente es utilizar el comandospanningtree vlan id-vlanpriority valor del modo de configuración global. Este comando da un control más detallado del valor de prioridad del puente (CISCO 2013). El valor de prioridad se configura en incrementos de 4096 entre 0 y 61440. En el ejemplo, se asignó el valor de prioridad de puente 24576 al S3 mediante el comando spanning-tree vlan 1 priority 24576. Para verificar la prioridad del puente de un switch, utilice el comando show spanning-tree. En la figura 8, la prioridad del switch se estableció en 24576. Además, observe que el switch está designado como puente raíz para la instancia de árbol de expansión. Utilice el verificador de sintaxis de la figura 3 para configurar los switches S1, S2 y S3. Mediante el método 2 descrito anteriormente, configure el S3 de forma manual y establezca el valor de prioridad en 24576 para la VLAN 1. Mediante el método 1, configure el S2 como raíz secundaria

para la VLAN 1 y el S1 como raíz principal para la VLAN 1. Verifique la configuración con el comando show spanning-treeen el S1.

Configurar y verificar el BID

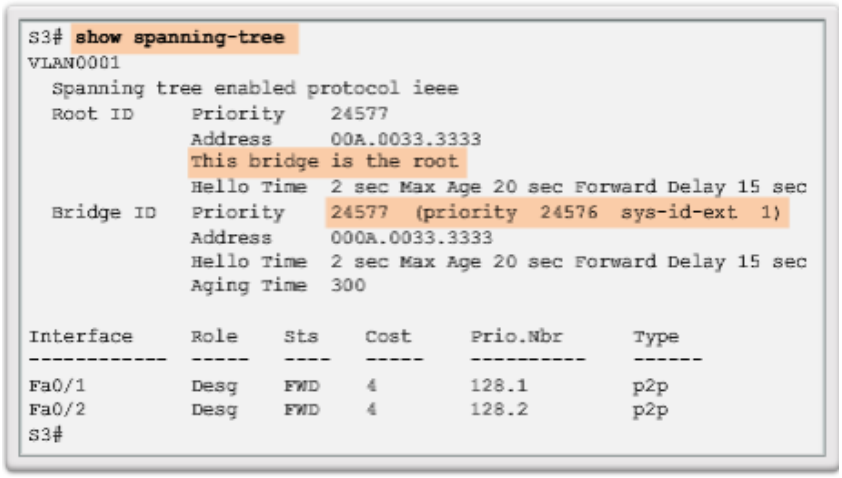

Figura 8. Configurar y verificar el BID
Fuente. (CISCO 2013)

3.2 PortFast y protección BPDU

PortFast es una característica de Cisco para los entornos PVST+. Cuando un puerto de switch se configura con PortFast, ese puerto pasa del estado de bloqueo al de reenvío de inmediato, omitiendo los estados de transición de STP 802.1D usuales (los estados de escucha y aprendizaje). Puede utilizar PortFast en los puertos de acceso para permitir que estos dispositivos se conecten a la red inmediatamente, en lugar de esperar a que STP IEEE 802.1D converja en cada VLAN (CISCO 2013). Los puertos de acceso son puertos conectados a una única estación de trabajo o a un servidor. En una configuración de PortFast válida, nunca se deben recibir BPDU, ya que esto indicaría que hay otro puente o switch conectado al puerto, lo que podría

causar un bucle de árbol de expansión. Los switches Cisco admiten una característica denominada “protección BPDU” (Stp 2010). Cuando se habilita, la protección BPDU coloca al puerto en estado deshabilitado por error al recibir una BPDU. Esto desactiva el puerto completamente. La característica de protección BPDU proporciona una respuesta segura a la configuración no válida, ya que se debe volver a activar la interfaz de forma manual. La tecnología Cisco PortFast es útil para DHCP. Sin PortFast, un equipo puede enviar una solicitud de DHCP antes de que el puerto se encuentre en estado de enviar e impedirle al host la posibilidad de obtener una dirección IP utilizable y cualquier otra información. Debido a que PortFast cambia el estado a enviar de manera inmediata, el equipo siempre obtiene una dirección IP utilizable.

3.3 Balanceo de carga de PVST+

En la topología de la figura a continuación, se muestran tres switches conectados mediante enlaces troncales 802.1Q. Hay dos VLAN, 10 y 20, que se enlazan de forma troncal a través de estos enlaces. El objetivo es configurar el S3 como puente raíz para la VLAN 20 y el S1 como puente raíz para la VLAN 10. El puerto F0/3 en el S2 es el puerto de reenvío para la VLAN 20 y el puerto de bloqueo para la VLAN 10. El puerto F0/2 en el S2 es el puerto de reenvío para la VLAN 10 y el puerto de bloqueo para la VLAN 20. Además de establecer un puente raíz, también es posible establecer uno secundario (CISCO 2013). Un puente raíz secundario es un switch que se puede convertir en puente raíz para una VLAN si falla el puente raíz principal. Si se tiene en cuenta que los otros puentes de la VLAN retienen su prioridad de STP predeterminada, este switch se convierte en el puente raíz en el caso de producirse una falla en el puente raíz principal. Los pasos para configurar PVST+ en esta topología de ejemplo son los

siguientes (Cinkler et al. 2005): Paso 1. Seleccionar los switches que desea como puentes raíz principal y secundario para cada VLAN. Por ejemplo, en la figura 1, el S3 es el puente principal y el S1 es el puente secundario para la VLAN 20. Paso 2. Configure el switch como puente principal para la VLAN mediante el comando spanning-tree vlannumber root primary, como se muestra en la figura 2. Paso 3. Configure el switch como puente secundario para la VLAN mediante el comando spanning-tree vlannumber root secondary. Otra forma de especificar el puente raíz es establecer la prioridad de árbol de expansión de cada switch en el menor valor, de modo que se seleccione el switch como puente principal para la VLAN asociada. Observe que, en la figura 2, el S3 está configurado como puente raíz principal para la VLAN 20 y el S1 está configurado como puente raíz principal para la VLAN 10 (CISCO 2013). El S2 mantuvo la prioridad de STP predeterminada. En la ilustración, también se observa que el S3 está configurado como puente raíz secundario para la VLAN 10 y el S1 está configurado como puente raíz secundario para la VLAN 20. Esta configuración habilita el balanceo de carga de árbol de expansión, en el que el tráfico de la VLAN 10 pasa por el S1 y el de la VLAN 20 pasa por el S3. Como se muestra en la figura 3, otra forma de especificar el puente raíz es establecer la prioridad de árbol de expansión de cada switch en el menor valor, de modo que se seleccione el switch como puente principal para la VLAN asociada. Se puede establecer la prioridad de switch para cualquier instancia de árbol de expansión (Stp 2010). Esta configuración afecta la posibilidad de que un switch se elija puente raíz. Un valor menor provoca el aumento de la probabilidad de que el switch sea seleccionado. El rango varía entre 0 y 61440 en incrementos de 4096; el resto de los valores se descarta. Por ejemplo, un valor de prioridad válido sería 4096 x 2 = 8192. Como se muestra en la figura 4, el comando show spanning-tree active solo muestra los detalles de configuración de árbol de expansión para las interfaces activas. El resultado que se

muestra pertenece al S1 configurado con PVST+. Existen varios parámetros de comandos del IOS de Cisco relacionados con el comando show spanning-tree. En la figura 5, el resultado muestra que la prioridad de la VLAN 10 es 4096, la más baja de las tres prioridades de VLAN respectivas. Utilice el verificador de sintaxis de la figura 6 para configurar y verificar el árbol de expansión para el S1 y el S3.

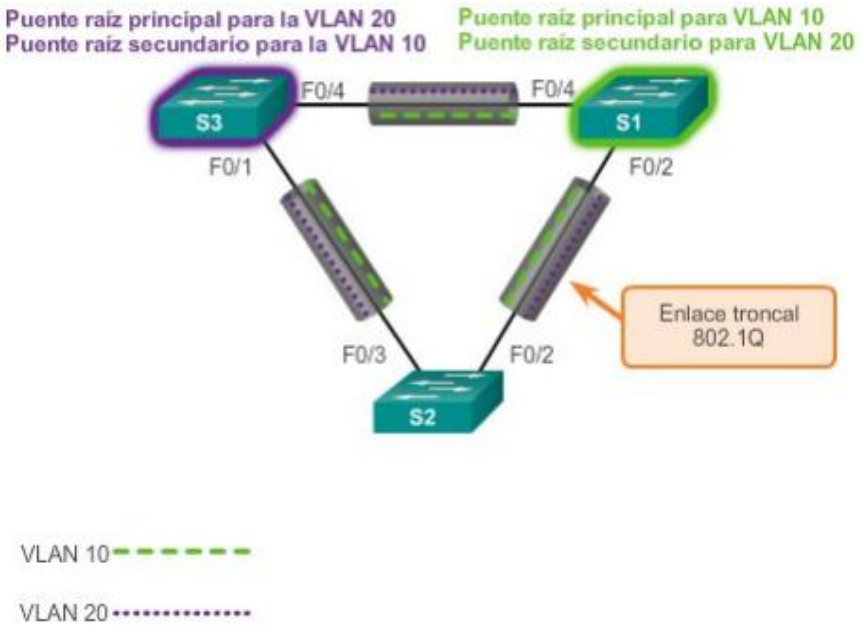

Figura 9. Topología PVST+
Fuente. (Anon n.d.)

La configuración seria de la siguiente manera

S1(config)# spanning-tree vlan 10 root primary

S1(config)# spanning-tree vlan 20 root secondary

S1(config)# spanning-tree vlan 1 priority 0

S1(config)# end

Capítulo 4. Consecuencias y solución frente a las fallas del árbol de expansión

En la mayoría de los protocolos, una falla significa que se pierde la funcionalidad que proporcionaba el protocolo. Existen dos tipos de falla en STP.

Es posible que STP bloquee por error los puertos que se deberían haber colocado en estado de reenvío. Se puede perder la conectividad para el tráfico que normalmente pasaría por este switch, pero el resto de la red no se ve afectada(Ibanez 2005).

El segundo tipo de falla es mucho más perjudicial, como se muestra en la figura 10. Esta falla se produce cuando STP pasa uno o más puertos al estado de reenvío por error. Recuerde que el encabezado de las tramas de Ethernet no incluye un campo TTL, lo que significa que los switches continúan reenviando indefinidamente cualquier trama que entre en un bucle de puente. Las únicas excepciones son las tramas que tienen la dirección de destino registrada en la tabla de direcciones MAC de los switches. Estas tramas simplemente se reenvían al puerto asociado a la dirección MAC y no ingresan a ningún bucle (CISCO 2013).

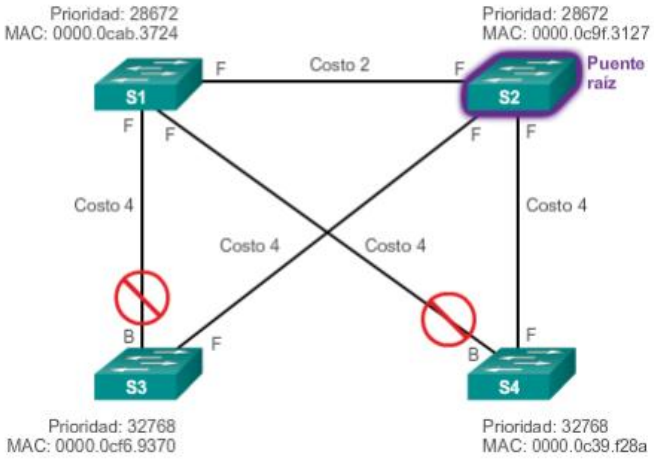

Figura 10. Falla de STP
Fuente. (CISCO 2013)

Sin embargo, cualquier trama que un switch use para saturar los puertos ingresa al bucle

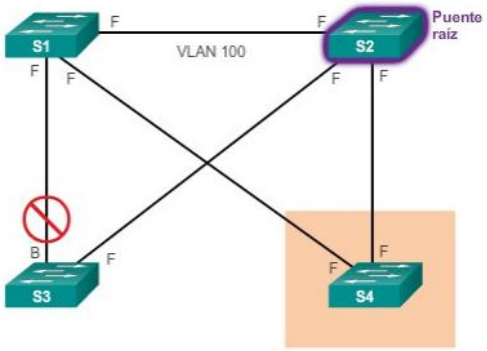

Figura 11. Transición errónea al estado de reenvió
Fuente. (CISCO 2013)

Esto puede incluir difusiones, multidifusiones y unidifusiones con una dirección MAC de destino desconocida globalmente. ¿Cuáles son las consecuencias y los síntomas correspondientes de la falla de STP?

La carga de todos los enlaces en la LAN conmutada comienza a aumentar rápidamente a medida que ingresan cada vez más tramas al bucle. Este problema no se limita a los enlaces que forman el bucle, sino que además afecta al resto de los enlaces en el dominio conmutado, dado que las tramas saturan todos los enlaces. Cuando la falla del árbol de expansión se limita a una única VLAN, solo los enlaces de esa VLAN se ven afectados. Los switches y los enlaces troncales que no transportan esa VLAN funcionan con normalidad. Si la falla del árbol de expansión creó un bucle de puente, el tráfico aumenta exponencialmente. Los switches saturan varios puertos con las difusiones. Esto crea copias de las tramas cada vez que los switches las reenvían (CISCO 2013).

Las CPU se acercan al 100% de utilización mientras intentan procesar una carga de tráfico del plano de control en constante aumento. En muchos casos, el primer indicio de esta tormenta de difusión en proceso es que los routers o los switches de capa 3 informan fallas en el plano de control y que están funcionando con una elevada carga de CPU. Los switches experimentan modificaciones frecuentes en la tabla de direcciones MAC. Si existe un bucle, es posible que un switch vea que una trama con determinada dirección MAC de origen ingresa por un puerto y que después vea que otra trama con la misma dirección MAC de origen ingresa por otro puerto una fracción de segundo más tarde. Esto provoca que el switch actualice la tabla de direcciones MAC dos veces para la misma dirección MAC. Debido a la combinación de una carga muy alta en todos los enlaces con el funcionamiento de las CPU del switch a la carga máxima, por lo general, no se puede llegar a estos dispositivos.

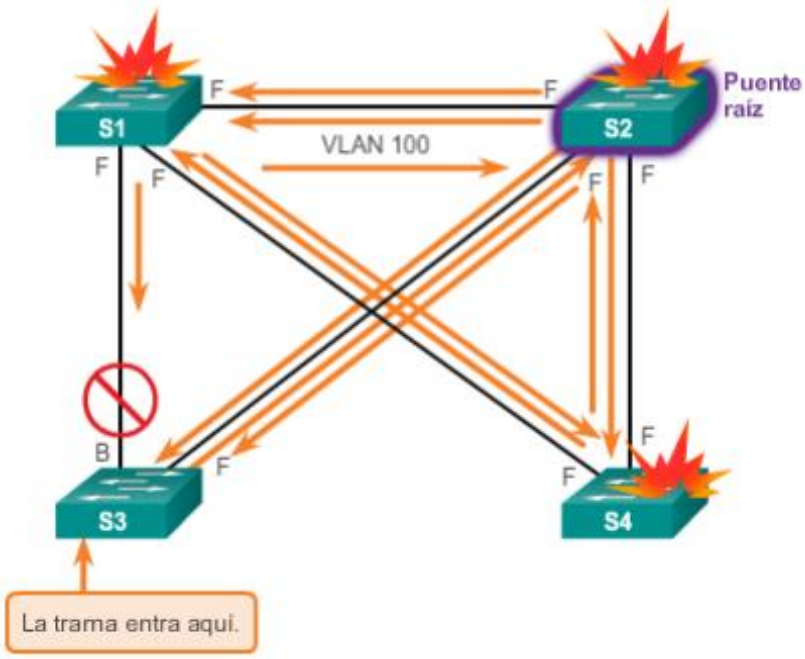

Figura 12. Consecuencias de la falla de STP
Fuente. (CISCO 2013)

4.1 Reparación De Un Problema Del Árbol De Expansión

Una forma de corregir la falla del árbol de expansión es eliminar de manera manual los enlaces redundantes en la red conmutada, ya sea físicamente o mediante la configuración, hasta eliminar todos los bucles de la topología (CISCO 2013). Cuando se rompen los bucles, las cargas de tráfico y de CPU deberían disminuir a niveles normales, y la conectividad a los dispositivos debería restaurarse. Si bien esta intervención restaura la conectividad a la red, el proceso de resolución de problemas no finaliza aquí. Se eliminó toda la redundancia de la red conmutada, y ahora se deben restaurar los enlaces redundantes. Si no se resolvió la causa subyacente de la falla del árbol de expansión, es probable que al restaurar los enlaces redundantes se desate una nueva tormenta de difusión. Antes de restaurar los enlaces redundantes, determine y corrija la causa de

la falla del árbol de expansión. Controle atentamente la red para asegurarse de que se haya resuelto el problema.

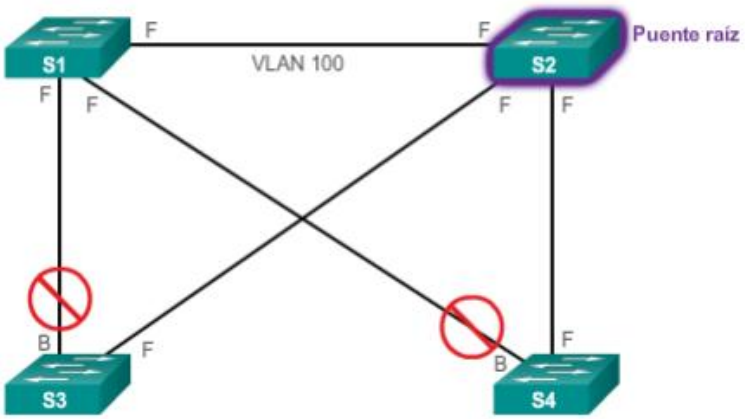

Figura 13. Reparación de un problema del árbol de expansión
Fuente. (CISCO 2013)

4.2 Limitaciones del Gateway predeterminado

Los protocolos de árbol de expansión permiten la redundancia física en una red conmutada. Sin embargo, los hosts en la capa de acceso de una red jerárquica también se benefician de los gateways predeterminados alternativos. Si falla un router o una interfaz del router (que funciona como gateway predeterminado), los hosts configurados con ese gateway predeterminado quedan aislados de las redes externas. Se necesita un mecanismo para proporcionar gateways predeterminados alternativos en las redes conmutadas donde hay dos o más routers conectados a las mismas VLAN. Nota: a los efectos del análisis de la redundancia de los routers, no existe ninguna diferencia funcional entre un switch multicapa y un router en la capa de distribución. En la práctica, es común que un switch multicapa funcione como gateway predeterminado para cada VLAN en una red conmutada. Este análisis se centra en la funcionalidad del routing,

independientemente del dispositivo físico que se utilice (CISCO 2013). En una red conmutada, cada cliente recibe solo un gateway predeterminado. No hay forma de configurar un gateway secundario, incluso si existe una segunda ruta que transporte paquetes fuera del segmento local. En la figura 14, el R1 es el responsable de enrutar los paquetes de la PC1. Si el R1 deja de estar disponible, los protocolos de routing pueden converger de forma dinámica. Ahora, el R2 enruta paquetes de redes externas que habrían pasado por el R1. Sin embargo, el tráfico de la red interna asociado al R1, incluido el tráfico de las estaciones de trabajo, de los servidores y de las impresoras que se configuraron con el R1 como gateway predeterminado, aún se envía al R1 y se descarta. Por lo general, las terminales se configuran con una única dirección IP para el gateway predeterminado (Stp 2010). Esta dirección no se modifica cuando cambia la topología de la red. Si no se puede llegar a esa dirección IP de gateway predeterminado, el dispositivo local no puede enviar paquetes fuera del segmento de red local, lo que lo desconecta completamente del resto de la red. Aunque exista un router redundante que sirva como puerta de enlace predeterminada para ese segmento, no hay un método dinámico para que estos dispositivos puedan determinar la dirección de una nueva puerta de enlace predeterminada.

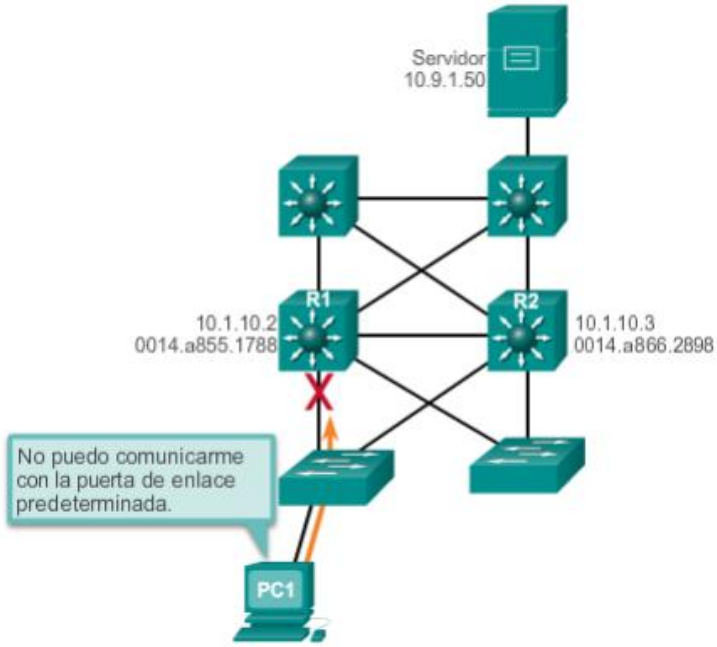

Figura 14. Limitaciones del gateway predeterminado
Fuente. (CISCO 2013)

Capítulo 5. Topología propuesta CON SWTICH 2950

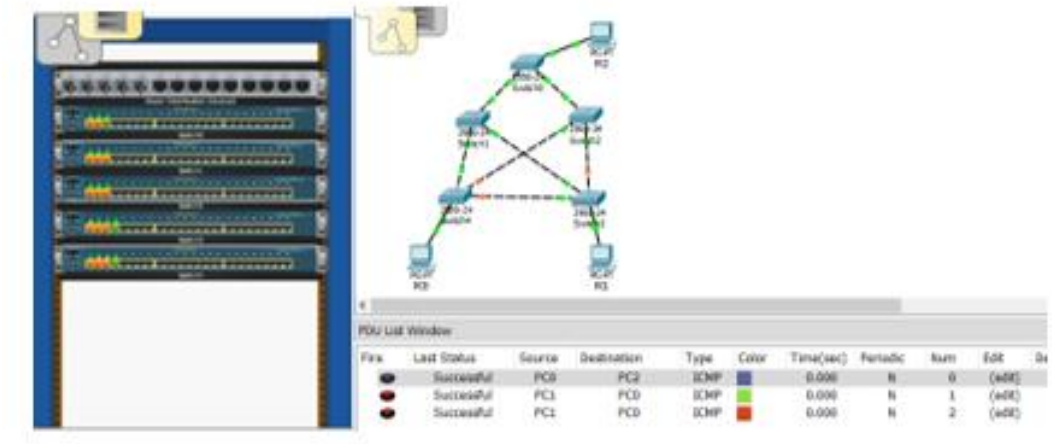

Figura 15. Topología Propuesta con switch 2950
Fuente. Autor del proyecto

De acuerdo a la topología propuesta, procedemos a visualizar a través del comando show spanning-tree el root ID y la prioridad

Para el switch 0

Switch#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0001.63C0.3892

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0001.63C0.3892

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------- ---- --- --------- -------- --------------------------------

Fa0/1 Desg FWD 19 128.1 P2p

Fa0/2 Desg FWD 19 128.2 P2p

Fa0/3 Desg FWD 19 128.3 P2p

Para el switch 1

Switch#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0001.63C0.3892

Cost 19

Port 2(FastEthernet0/2)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0001.6480.DBCB

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------- ---- --- --------- -------- --------------------------------

Fa0/1 Desg FWD 19 128.1 P2p

Fa0/2 Root FWD 19 128.2 P2p

Fa0/3 Desg FWD 19 128.3 P2p

Para el switch 4

Switch#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0001.63C0.3892

Cost 38

Port 1(FastEthernet0/1)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 00E0.A3D3.4981

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------- ---- --- --------- -------- --------------------------------

Fa0/3 Altn BLK 19 128.3 P2p

Fa0/2 Altn BLK 19 128.2 P2p

Fa0/4 Desg FWD 19 128.4 P2p

Fa0/1 Root FWD 19 128.1 P2p

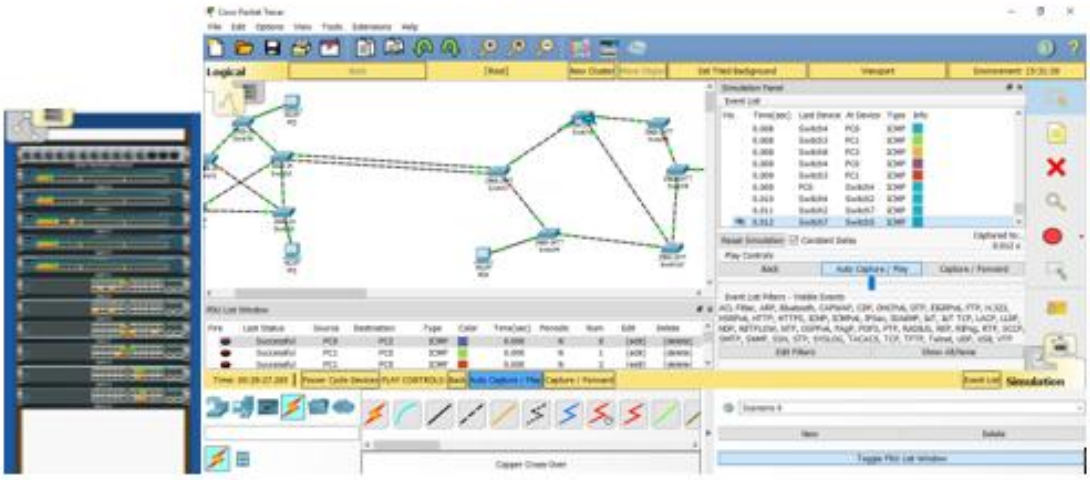

Figura 16. Agregación de dos segmentos a la Intranet
Fuente. Autor del proyecto

Conclusiones

A través del curso de profundización ofrecido por la Universidad Francisco de Paula Santander Ocaña soportado por el laboratorio de redes y telecomunicaciones, se adquirió diferentes competencias enmarcadas en un contexto teórico-práctico aplicable al diseño y configuración de dispositivos Cisco.

Se pueden producir situaciones en las que STP no se haya tenido en cuenta en el diseño y la implementación de la red, o en las que se hayan tenido en cuenta y se lo haya implementado antes de que la red se expandiera y sufriera modificaciones a gran escala. En dichas situaciones, es importante saber analizar la topología STP real en la red en funcionamiento. Una gran parte de la resolución de problemas implica comparar el estado real de la red con el estado que se espera de esta y detectar las diferencias para reunir pistas acerca del problema que se debe resolver.

Mediante la investigación realizada se sugiere a la división de sistemas implementar este tipo de tecnologías, con el ánimo de ayudar a mejorar los cuellos de botella que se generan en la horas picos, y hacen que la intranet de la UFPS Ocaña se muy lenta, y de una u otra manera evitar que los técnicos tengan que desconectar los cables de backup.

Referencias

Anon, 2.3.1.4 Balanceo de carga de PVST+. Available at: http://static-course-assets.s3.amazonaws.com/ScaN50ES/course/module2/2.3.1.4/2.3.1.4.html [Accessed March 17, 2018a].

Anon, Understanding Multiple Spanning Tree Protocol (802.1s) - Cisco. Available at: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24248-147.html [Accessed March 17, 2018b].

Cinkler, T. et al., 2005. Optimizing QoS aware ethernet spanning trees. *2005 1st International Conference on Multimedia Services Access Networks, MSAN05*, 2005(c), pp.30–34.

CISCO, 2013. Cisco Networking Academy - Cisco Systems Cisco Networking Academy. *Cisco Systems*, pp.1–2. Available at: https://www.netacad.com/es/group/landing/v2/manage/ [Accessed March 17, 2018].

CISCO NETACAD, Escalamiento de redes. Available at: https://static-course-assets.s3.amazonaws.com/ScaN503/es/index.html#2.5.1.2 [Accessed January 21, 2018].

Ibanez, G., 2005. Contribucion al Diseno de Redes Campus Ethernet Autoconfigurables. *PhD Thesis*, p.255.

Ingenieros, E.S. De, 2007. Evaluación de alternativas en la aplicación de Spanning Tree Protocol.

Kern, A., Moldován, I. & Cinkler, T., 2006. Scalable tree optimization for QoS ethernet. *Proceedings - International Symposium on Computers and Communications*, pp.578–583.

Stp, L.G., 2010. Mejoras del protocolo de árbol de expansión usando las funciones de Loop Guard y BPDU Skew detección de desviación.

Alejandro. (11 de diciembre de 2016). *Protegemipc*. Obtenido de https://protegermipc.net/2016/10/11/que-es-y-como-funciona-un-arbolexpvpn/

ALONSO MONTES, José L., ALMOROX GONZÁLEZ, Pablo, RODRÍGUEZ SALAZAR, José A. Wi-Fi: El diferente uso del espectro en EEUU y Europa. Tecnología y sociedad [CD-ROM], ed. 149, feb-mar 2010.

FOROUZAN. Transmisión de datos y redes de comunicación. 2ª edición. México: McGraw - hill. 2002. ISBN: 8448133900. 453p.

MADRID MOLINA, Juna Manuel. Análisis Seguridad en redes inalámbricas 802.11, Universidad Icesi. SISTEMAS & TELEMÁTICA. 2004.

MILLÁN, Andrés F., DAZA Ronald., CAMPIÑO, James. Estudio de los puntos de acceso inalámbricos 802.11 en la ciudad de Cali usando las técnicas WAR-X [CD-ROM], Santiago de Cali. SISTEMAS & TELEMÁTICA, mar. 2006.

TANENBAUM, Andrew S. Redes de computadoras. 4ª edición. España: Pearson. 2003. ISBN 9789702601623. 786p.

Política de Territorios Digitales. 2011. [Citado 19 de septiembre de 2015] [En Línea] Disponible en http://es.slideshare.net/frajaro/territorios-digitales-hacia-territorios-del-conocimiento-7079003

Anon, 2.3.1.4 Balanceo de carga de PVST+. Available at: http://static-course-assets.s3.amazonaws.com/ScaN50ES/course/module2/2.3.1.4/2.3.1.4.html [Accessed March 17, 2018a].

Anon, Understanding Multiple Spanning Tree Protocol (802.1s) - Cisco. Available at: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24248-147.html [Accessed March 17, 2018b].

Cinkler, T. et al., 2005. Optimizing QoS aware ethernet spanning trees. *2005 1st International Conference on Multimedia Services Access Networks, MSAN05*, 2005(c), pp.30–34.

CISCO, 2013. Cisco Networking Academy - Cisco Systems Cisco Networking Academy. *Cisco Systems*, pp.1–2. Available at: https://www.netacad.com/es/group/landing/v2/manage/ [Accessed March 17, 2018].

CISCO NETACAD, Escalamiento de redes. Available at: https://static-course-

assets.s3.amazonaws.com/ScaN503/es/index.html#2.5.1.2 [Accessed January 21, 2018].

Ibanez, G., 2005. Contribucion al Diseno de Redes Campus Ethernet Autoconfigurables. *PhD Thesis*, p.255.

Ingenieros, E.S. De, 2007. Evaluación de alternativas en la aplicación de Spanning Tree Protocol.

Kern, A., Moldován, I. & Cinkler, T., 2006. Scalable tree optimization for QoS ethernet. *Proceedings - International Symposium on Computers and Communications*, pp.578–583.

Stp, L.G., 2010. Mejoras del protocolo de árbol de expansión usando las funciones de Loop Guard y BPDU Skew detección de desviación.

Apéndice

Ficha Técnica Switch CATALYST 2950 Series - WS-C2950-24

Figura 17. Switch serie 2950

Fuente. Autor del proyecto

La serie Cisco Catalyst 2950 de conmutadores Ethernet inteligentes es una línea de dispositivos de configuración fija, apilables e independientes, que proporcionan conectividad Fast Ethernet y Gigabit Ethernet a velocidades de cable. Es una familia de switches de Cisco con los precios más asequibles.

General

Tipo de dispositivo	Conmutador - 24 puertos - Gestionado
Tipo incluido	Sobremesa 1U
Subtipo	Fast Ethernet
Puertos	24 x 10/100
Tamaño de tabla de dirección MAC	8K de entradas
Protocolo de gestión remota	SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, HTTP
Método de autentificación	RADIUS, TACACS+, Secure Shell v.2 (SSH2)
Características	Control de flujo, capacidad duplex, concentración de enlaces, soporte VLAN, snooping IGMP, soporte para Syslog, Cola Round Robin (WRR) ponderada, actualizable por firmware
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s
Memoria Flash	8 MB Flash
Indicadores de estado	Velocidad de transmisión del puerto, modo puerto duplex, ancho de banda utilización %, alimentación, tinta OK, estado, enlace/actividad

Expansión / Conectividad

Interfaces	1 x consola - RJ-45 - gestión 24 x 100Base-TX - RJ-45

Alimentación

Dispositivo de alimentación	Fuente de alimentación eléctrica
Voltaje necesario	CA 120/230 V (50/60 Hz)
Consumo eléctrico en funcionamiento	30 vatios
Características	Contector de sistema de alimentación redundante (RPS)

Diverso

Cumplimiento de normas	Certificado FCC Clase A, CISPR 22 clase A, BSMI CNS 13438 Class A, EN 60950, equipo de TI de clase A según el VCCI, IEC 60950, CSA 22.2 No. 950, EN55022 clase A, UL 60950, ACA TS001, AS/NZS 3260, FCC Part 15, MIC

Software / Requisitos del sistema

Software incluido	Standard Image (SI) Software

Medidas y peso

Anchura	44.5 cm
Profundidad	24.2 cm
Altura	4.4 cm
Peso	3 kg

Garantía del fabricante

Servicio y mantenimiento	Garantía limitada - de por vida

Parámetros de entorno

Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	45 °C
Ámbito de humedad de funcionamiento	10 - 85%
Altitud máxima de funcionamiento	3 km

FICHA TÉCNICA CISCO CATALYST 2960-PLUS 24PC-S - WS-C2960+24PC-S

Figura 18. Switch serie 2960

Figura. Autor del proyecto

Los switches Cisco Catalyst 2960 admiten voz, video, datos y acceso sumamente seguro. También brindan administración escalable para adaptarse a sus cambiantes necesidades comerciales.

- Los switches Cisco Catalyst de las series 2960 ofrecen funciones de switching sobresalientes
- Las capacidades para comunicaciones de datos, inalámbricas y de voz le permiten instalar una sola red para todas sus necesidades de red y comunicación
- Seguridad avanzada como servicios de identidad y control de acceso sofisticado para proteger sus recursos esenciales
- Funciones de redundancia y recuperabilidad para proteger en todo momento la disponibilidad de sus aplicaciones críticas

General

Tipo de dispositivo	Conmutador - 24 puertos - Gestionado
Tipo incluido	Montaje en rack 1U
Subtipo	Fast Ethernet
Puertos	24 x 10/100 (PoE) + 2 x Gigabit SFP combinado
Alimentación por Ethernet (PoE)	PoE
Presupuesto PoE	370 W
Rendimiento	Capacidad de conmutación: 16 Gbps Rendimiento de reenvío (tamaño de paquete de 64 bytes): 6.5 Mpps
Capacidad	VLAN activas: 64
Admite carcasa Jumbo	9018 bytes
Protocolo de gestión remota	SNMP 1, RMON 1, RMON 2, Telnet, SNMP 3, SNMP 2c, CLI
Método de autentificación	RADIUS, TACACS+
Características	Capacidad duplex, soporte BOOTP, soporte ARP, soporte VLAN, soporte para Syslog, soporte DiffServ, soporte IPv6, admite Spanning Tree Protocol (STP), admite Rapid Spanning Tree Protocol (RSTP), admite Multiple Spanning Tree Protocol (MSTP), snooping DHCP, soporte de Port Aggregation Protocol (PAgP), soporte de Trivial File Transfer Protocol (TFTP), Quality of Service (QoS), Dynamic ARP Inspection (DAI), tecnología Cisco EnergyWise, Shaped Round Robin (SRR), con LLDP, relé DHCP, Protocolo de control de adición de enlaces (LACP), MAC Address Notification, Management Information Base (MIB), Class of Service (CoS), admite DiffServ Code Point (DSCP)
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah, IEEE 802.1ab (LLDP)
Memoria RAM	128 MB
Memoria Flash	64 MB
Indicadores de estado	Velocidad de transmisión del puerto, modo puerto duplex, sistema, estado, RPS (suministro de energía redundante), PoE

Expansión / Conectividad

Interfaces	24 x 100Base-TX - RJ-45 - PoE - 15.4 W 2 x - SFP - subida 2 x 1000Base-T - RJ-45 - subida

Alimentación

Dispositivo de alimentación	Fuente de alimentación eléctrica
Voltaje necesario	CA 120/230 V (50/60 Hz)
Consumo eléctrico en funcionamiento	35 vatios
Características	Contector de sistema de alimentación redundante (RPS)

Diverso

MTBF (tiempo medio entre errores)	381,000 horas
Cumplimiento de normas	CISPR 22 clase A, BSMI CNS 13438 Class A, CISPR 24, EN 61000-3-2, EN 61000-3-3, EN55024, EN55022 clase A, AS/NZS 60950-1, ICES-003 clase A, FCC CFR47 Part 15, UL 60950-1 Second Edition, Directive 2004/108/EC, CSA C22.2 No. 60950-1 Second Edition, EN 60950-1 Second Edition, IEC 60950-1 Second Edition, Directive 2006/95/EC, VCCI Class A, KN24, KN22 Class A, EN 300386, RoHS 2011/65/EU

Software / Requisitos del sistema

Software incluido	Cisco IOS LAN Lite

Medidas y peso

Anchura	45 cm
Profundidad	33.2 cm
Altura	4.4 cm
Peso	5.4 kg

Garantía del fabricante

Servicio y mantenimiento	Garantía limitada - sustitución de piezas con antelación - de por vida - tiempo de respuesta: el siguiente día laborable Soporte técnico - asesoramiento - 90 días

Parámetros de entorno

Temperatura mínima de funcionamiento	-5 °C
Temperatura máxima de funcionamiento	40 °C
Ámbito de humedad de funcionamiento	10 - 95% (sin condensación)
Temperatura mínima de almacenamiento	-25 °C
Temperatura máxima de almacenamiento	70 °C
Ámbito de humedad de almacenamiento	10 - 95% (sin condensación)

- Un sistema de comunicación todo en uno Gracias a sus capacidades para datos, conexión inalámbrica y voz, cuando esté listo para implementar estos servicios tendrá una sola red capaz de sustentar sus necesidades comerciales.
- Inteligencia Asigne prioridad al tráfico de voz o al intercambio de datos para que la entrega de información concuerde con sus requisitos empresariales.

- Seguridad mejorada Proteja información importante, mantenga a los usuarios no autorizados fuera de la red y mantenga un funcionamiento ininterrumpido.
- ConfiabilidadAproveche los métodos basados en estándares o el apilamiento FlexStack para aumentar la confiabilidad y para una rápida recuperación tras problemas. También puede añadir un suministro de alimentación redundante para mayor confiabilidad.
- Configuración sencillaUtilice Cisco Catalyst Smart Operations y Cisco Network Assistant para simplificar la configuración, las actualizaciones y la resolución de problemas.