

Prácticas recomendadas para la migración de varios árboles de extensión

Objetivo

El objetivo de este documento es proporcionarle las mejores prácticas al migrar a un árbol de extensión múltiple (MSTP). El uso de MSTP sobre otras variantes del árbol de extensión puede mejorar la eficacia y la fiabilidad de la red.

Requirements

- La necesidad de optimizar la capa 2 en un entorno de hardware mixto
 - Switches Cisco Small Business
 - Serie Sx250 ([Guía de administración](#))
 - Serie Sx300 ([Guía de administración](#))
 - Serie Sx350 ([Guía de administración](#))
 - Serie SG350X ([Guía de administración](#))
 - Serie Sx550X ([Guía de administración](#))
 - Switches Catalyst de Cisco
- Una comprensión funcional del árbol de expansión ([Más información](#))
- Wireshark (opcional)

Table Of Contents

1. [Terminología MSTP](#)
2. [Práctica recomendada n.º 1 - Validar la necesidad de migrar a MSTP](#)
3. [Práctica recomendada n.º 2 - Estrategias para la migración](#)
4. [Práctica recomendada n.º 3 - Práctica recomendada n.º 3 - Habilite los puertos punto a punto para utilizar PortFast](#)
5. [Práctica recomendada n.º 4: Habilitar la protección BPDU en los puertos de borde](#)
6. [Práctica recomendada n.º 5: asigne VLAN a MSTI, no al IST \(MST0\)](#)
7. [Práctica recomendada n.º 6: coloque todos los switches habilitados para MSTP en la misma región](#)
8. [Práctica recomendada n.º 7: niegue el puente raíz de CIST en la región principal de MST](#)
9. [Verificación de la migración - ¿Está esto en marcha?](#)
10. [Conclusión](#)

Estructura de esta guía

En esta guía se omiten pasos como el inicio de sesión en el dispositivo a través de SSH o la interfaz de administración; en su lugar, resaltaremos los comandos de núcleo. Cada práctica recomendada contendrá una subtarea en la que se describen los pasos adecuados para el hardware mixto de Cisco (grandes empresas y PYMES). Para ver las guías de configuración, vea los dos enlaces siguientes:

- [Configuración de MSTP en el switch SMB](#)
- [Configuración de MSTP en el Switch Catalyst](#)

Terminología MSTP

Esta sección está diseñada para proporcionarle un modelo mental accesible del protocolo en juego. Las definiciones son componentes de interconexión del protocolo MSTP. En los puntos secundarios figuran más detalles.

BPDU - Unidad de datos de protocolo de puente - Estas son tramas de multidifusión que contienen toda la información que un switch necesita para continuar funcionando.

Nota: que las asignaciones de instancia no están en la BPDU.

Región - (*Específica de MSTP*) - Una región resuelve el problema encontrado por otros tipos de STP que envían una BPDU por VLAN. Al igual que con Per Vlan Spanning Tree, el envío de tantas BPDU causa tensión en la carga de la CPU y, por lo tanto, dificulta el rendimiento de la red. En su lugar, con MSTP todas las VLAN se asignan a una sola región.

Instancia: Una instancia es una instancia de una tabla lógica de una VLAN, o de muchas VLAN, a una región determinada. Esta instancia luego se asigna a una zona. Como parte de la migración, deberá completar estos pasos.

La instancia predeterminada 0 (cero) es sinónimo de los siguientes términos *MST0*, *Árbol de expansión interno (IST)*.

Se hace referencia a las instancias creadas por usted como Instancias de árbol de extensión múltiple o MSTI.

Aquí es donde la buena documentación de las VLAN de su red le ahorrará complicaciones.

- Si una instancia falla, no afectará a otras instancias.

MSTI - Varias instancias de árbol de extensión - Contiene la instancia creada administrativamente. Estos mapeos están contenidos en lo que se conoce como "MRecord", visible a través de Wireshark. Los registros incluyen detalles necesarios para administrar la topología de la instancia.

IST - Árbol de expansión interno - es el registro de switches que participan en una zona MSTP. Los switches (no importa cuántos) contenidos dentro de una zona, se representan en áreas fuera de la zona como un único switch.

- **CST - Árbol de expansión común** - se compone de regiones MSTP que ejecutan su propio árbol de expansión tradicional. CST utiliza links entre los switches en el límite de la zona MSTP.

CIST - Árbol de expansión común e interno - Compuesto tanto por CST como por IST que atraviesa varias instancias basándose en un mapeo compartido de VLAN a la instancia.

Common and Internal Spanning Tree *no* es Common Spanning Tree.

Ahora que hemos establecido para quién es este artículo y las definiciones pertinentes, veamos las mejores prácticas.

Práctica recomendada n.º 1 - Validar la necesidad de migrar a MSTP

La primera práctica recomendada consiste en confirmar su necesidad de migrar a MSTP. La comprensión del rendimiento actual del árbol de extensión de la red es un factor clave en esta decisión. La migración a MSTP sería una opción excelente por algunos motivos, ya que introduce el uso compartido de la carga, lo que supone el mayor impacto en la eficacia de la red. Si el tráfico de capa 2 ha aumentado antes de lo previsto, el cambio a MSTP puede aumentar la utilidad/duración de su equipo a través de un mejor rendimiento. Otras consideraciones podrían ser:

El rendimiento STP existente no es satisfactorio - el tiempo de convergencia o la cantidad de BPDU transmitidas está causando problemas

Árbol de expansión de segmentos: reduce la carga de recursos en los switches contenidos en las regiones MSTP.

Entorno de hardware mixto: MSTP es un estándar abierto, lo que significa que es ideal para un entorno de proveedor mixto. Está ampliamente respaldada.

Nota: Un error común es que al migrar a un árbol de expansión múltiple debe asignar una VLAN por instancia.

Los sabores del árbol de expansión han surgido, con variaciones y giros en versiones anteriores. En comparación con Per VLAN Spanning Tree (PVST+), MSTP utiliza menos recursos (BPDUS, ciclos de CPU, tiempo de transmisión) al mantener instancias de Spanning Tree o versiones lógicas de Spanning Tree. El tráfico VLAN se habilita para fluir a través de los segmentos de capa 2 de una red. El reenvío para un puerto (y VLAN) también puede bloquearse para una VLAN diferente. Además, si se forma un bucle en una instancia, no afectará a las otras instancias.

Práctica recomendada n.º 2 - Estrategias para la migración

Una vez validada la necesidad de migrar, idealmente, la migración se logra con un tiempo de inactividad mínimo y se mantiene la conectividad existente. Una pequeña estrategia para hacer frente a la migración contribuirá en gran medida a garantizar una implantación sin contratiempos. Para ayudar con ese proceso, recomendamos los siguientes pasos tácticos.

1. *Documento, documento, documento:* el mantenimiento de notas detalladas reducirá el tiempo de migración y la posibilidad de que se produzcan errores.

Identifique y documente todos los puertos punto a punto o los puertos que conducen a otro switch o router.

Identifique y documente todos los puertos de borde o los puertos que conducen a un punto final como un PC o una impresora.

Definir qué VLAN participan en la migración

¡Los becarios son muy buenos en este paso!

Determine el orden de las operaciones de la red.

Tenga en cuenta cómo un cambio en un switch puede afectar a una VLAN diferente.

Programe el tiempo de inactividad de su red o realice la migración el fin de semana.

Inicie la migración en el núcleo de su red y trabaje hasta la distribución y, a continuación, la capa de acceso.

Práctica recomendada n.º 3 - Habilite los puertos punto a punto para utilizar PortFast

Esta mejor práctica, y la siguiente, hacen buen uso de toda esa documentación del puerto. Los administradores definen un parámetro opcional en los puertos de borde mediante la función PortFast. PortFast evita que el Spanning Tree se ejecute en ese puerto. Los puertos orientados de switch a equipo podrían incluir un servidor, una estación de trabajo y un router. La intención es que ese puerto nunca conecte la red con otro conjunto de puertos abiertos. Lo que podría causar loops si el switch recibiera una BPDU superior. Dado que los puertos que se conectan a una red realizan un cálculo STP en el puerto, puede ahorrar tiempo y carga de CPU asignando el estado de bloqueo antes de tiempo. Permite al puerto pasar rápidamente a un estado de envío - reenvío BPDU. Porque se le ha asignado un estado con antelación.

Nota: Asegúrese de que los puertos de los switches estén configurados para la transmisión de dúplex completo.

Los siguientes pasos se dividirán entre los switches SMB (CLI + GUI) y los switches catalyst empresariales (CLI).

Habilitación de Portfast en Catalyst Switch - CLI

Los comandos CLI se presentan primero con la sintaxis, seguidos de un ejemplo de un comando activo. Después del # se ha agregado un espacio adicional para facilitar un poco el realce para copiar > pegar. El texto resaltado en azul indica las variables que se reemplazarán por los detalles contextuales de la red. También tenga en cuenta para la brevedad que los únicos comandos de elevación de privilegios que utilizamos serán para la configuración MSTP.

```
Catalyst(config)# interface [range(opcional)] [port-id]
Catalyst(config-if)# spanning-tree portfast [auto]
```

```
Catalyst(config)# interface range fa0/1 - 24
Catalyst(config-if)# spanning-tree portfast auto
```

Habilitación de Portfast en el Switch SMB - CLI

```
SMBswitch(config)# interfaz [rango(opcional)] [port-id]
SMBswitch(config-if)# spanning-tree portfast
```

```
SMBswitch(config)# rango de interfaz gi1-15
SMBswitch(config-if)# spanning-tree portfast
```

Habilitación de Portfast en el Switch SMB - GUI

Una advertencia a tener en cuenta es que la GUI de los switches SMB utiliza un sinónimo para *PortFast* - es conocido como *Fast Link*.

Paso 1. Haga clic en **Spanning Tree > STP Interface Settings**.

Paso 2. Seleccione una **interfaz** y haga clic en el **botón Editar**.

Paso 3. Haga clic en **Enable Fast Link** .

Nota: Recuerde aplicar los cambios y escribir la configuración en ejecución en la configuración de inicio.

Práctica recomendada n.º 4: Habilitar la protección BPDU en los puertos de borde

Esta práctica recomendada es una extensión de la anterior. Si un puerto habilitado para la protección BPDU ve que el puerto que recibe cualquier BPDU superior que cambie la topología, inmediatamente cierra el puerto a través del estado *err-disable*. Para ello, tendría que acceder al switch y resolver la situación.

Nota: Puede parecer una de esas prácticas recomendadas que puede omitir. ¿Podrías salirte con la tuya? Tal vez, pero por el bien de tu futuro, hazlo así. Un switch errante traído a la red y bombeando las BPDU erróneas podría potencialmente derribar su red.

Habilitación de la Protección BPDU en el Switch Catalyst - CLI

```
Catalyst(config)# interface [range(opcional)] [port-id]
Catalyst(config-if)# spanning-tree bpduguard enable
```

```
Catalyst(config)# interface range fa0/1 - 24
Catalyst(config-if)# spanning-tree bpduguard enable
```

Habilitación de la Protección BPDU en el Switch SMB - CLI

```
SMBswitch(config)# interface [range(opcional)] [port-id]
SMBswitch(config-if)# spanning-tree bpduguard enable
```

```
SMBswitch(config)# interface range fa0/1 - 24
SMBswitch(config-if)# spanning-tree bpduguard enable
```

Habilitación de la Protección BPDU en el Switch SMB - GUI

Paso 1. Inicie sesión en la utilidad de configuración web para elegir **Spanning Tree > STP Interface Settings**. Se abre la página STP Interface Settings (Parámetros de interfaz STP).

Paso 2. Elija el tipo de **interfaz** que desea editar en la lista desplegable Tipo de interfaz.

Paso 3. Haga clic en **Ir** para mostrar sólo puertos o LAG en la página.

Paso 4. Haga clic en el botón de **radio** del puerto o LAG conectado al otro switch y haga clic en **Editar**. Aparece la ventana Edit STP Interface .

Paso 5. Haga clic en la casilla de verificación BPDU Guard Guard **Enable** que corresponde al tipo de interfaz deseado en el campo *Interface*.

Práctica recomendada n.º 5: asigne VLAN a MSTI, no al IST (MST0)

Ahora los puertos saben cuál es su función apropiada, pasemos a la asignación de instancias. Para obtener los mejores resultados, limite la cantidad de instancias que cree; tenga en cuenta que hay algunos matices. Esto es contrario a las prácticas recomendadas y podría disuadir a un ingeniero de MSTP como solución. Puede tener consideraciones de diseño de red válidas para varias instancias, pero tenga en cuenta que la mejor práctica es tener una sola instancia. Decida qué VLAN se asignarán a las instancias. A continuación, elija un nombre de configuración y un número de revisión que serán comunes a todos los switches de la red.

Nota: Cuando edita las asignaciones de VLAN MSTI, se reinicia MSTP.

Asignación de VLAN en Catalyst Switch - CLI

```
Catalyst(config)# spanning-tree mst configuration
Catalyst(config-mst)# instance [instance-id] vlan [vlan-range]
```

```
Catalyst(config)# spanning-tree mst configuration
Catalyst(config-mst)# instance 1 vlan 1-11
```

Asignación de VLAN en el switch SMB - CLI

```
SMBswitch(config)# configuración de spanning-tree mst
SMBswitch(config-mst)# instance [instance-id] vlan [vlan-range]
```

```
SMBswitch(config)# configuración de spanning-tree mst
SMBswitch(config-mst)# instancia 1 vlan 1-11
```

Asignación de VLAN a MSTI - GUI

Paso 1. Haga clic en **Spanning Tree > VLAN** para la Instancia MSTP.

La página *VLAN to MSTP Instance* contiene los campos siguientes:

- *ID de instancia de MST*: se muestran todas las instancias de MSTP.
- *VLANs*: se muestran todas las VLAN que pertenecen a la instancia de MST.

Paso 2. Para agregar una VLAN a una instancia de MSTP, seleccione la **instancia de MST** y haga clic en **Editar**.

- *ID de instancia de MST*: seleccione la instancia de MST.
- *VLAN*: defina las VLAN que se asignan a esta instancia de MST.
- *Acción*: defina si agregar (asignar) la VLAN a la instancia de MST o eliminarla.

Paso 3. Introduzca sus **parámetros**.

Paso 4. Haga clic en Apply (Aplicar). En este punto, se establecen las asignaciones de VLAN MSTP.

Práctica recomendada nº 6: coloque todos los switches habilitados para MSTP en la misma región

La mejor práctica es colocar tantos switches en una sola región como sea posible. No hay ventajas en segmentar la red en varias regiones. Al igual que con cualquier protocolo de routing y switching, requieren una forma de confirmar la pertenencia al protocolo. Las BPDUs enviadas permiten que un switch se reconozca como miembro de una región determinada. Para que el puente comprenda su pertenencia a una región determinada, debe compartir las siguientes configuraciones:

1. Nombre de región
2. Número de revisión
3. Resumen calculado a partir de la asignación de VLAN a instancia

Conexión del puente dentro de una región en el switch Catalyst - CLI

```
Catalyst(config)# spanning-tree mst [instance-id] root primary
```

```
Catalyst(config)# spanning-tree mst 5 root primary
```

Inicio del puente dentro de una región en el switch SMB - CLI

```
SMBswitch(config)# configuración de spanning-tree mst  
SMBswitch(config-mst)# instance [instance-id] vlan [vlan-range]  
SMBswitch(config-mst)# name [region-name]  
SMBswitch(config-mst)# revisión [revision-id]
```

```
SMBswitch(config)# configuración de spanning-tree mst  
SMBswitch(config-mst)# instancia 1 vlan 10-20  
SMBswitch(config-mst)# nombre región1  
SMBswitch(config-mst)# revisión 1
```

Inicio del puente dentro de una región en el switch para PYMES - GUI

La página Propiedades de MSTP se utiliza para definir en qué región se encuentra el switch. Para que los dispositivos estén en la misma región, deben tener el mismo nombre de región y el mismo valor de revisión.

Paso 1. Elija **Spanning Tree > MSTP Properties** en el menú.

Paso 2. Ingrese un **nombre** para la región MSTP en el campo *Region Name*. El nombre de la región define el límite lógico de la red. Todos los switches de una región MSTP deben tener el mismo nombre de región configurado.

Paso 3. Introduzca un **número de revisión** en el *campo Revisión*. Este es un número lógico que significa una revisión para la configuración MSTP. Todos los switches de una región MSTP deben tener el mismo número de revisión.

Paso 4. Introduzca el número máximo de **saltos** en el *campo Max Hops*. Max Hops especifica la duración de las BPDUs en los recuentos de saltos. Cuando un bridge recibe una BPDUs, disminuye el conteo de saltos en uno y reenvía la BPDUs con el nuevo conteo de saltos. Una vez que un

bridge recibe una BPDU con un conteo de saltos de cero, se descarta la BPDU.

Nota: El campo *IST Active* muestra la prioridad de puente y la dirección MAC del switch activo de la región. [Consulte el glosario para obtener información adicional.](#)

Paso 5. Haga clic en Apply (Aplicar).

Práctica recomendada n.º 7: niegue el puente raíz de CIST en la región principal de MST

Esta práctica recomendada forma parte del eje fundamental para mantener unida toda la migración. La idea es colocar el puente raíz para la topología MSTP - dentro de la región MSTP principal. Dada la práctica recomendada anterior que colocaba todas las VLAN dentro de la misma región, la selección de raíz es válida para todas las VLAN. Esto se logra a través de la función conocida como protección de raíz, que aplica la ubicación de raíz creada por usted. Cuando un bridge recibe una BPDU superior en un puerto activado de la protección raíz, inmediatamente colocará el puerto en el modo de escucha, a través del estado STP root-inconsistent. Esto evita el reenvío de sus BPDU inferiores, preservando así los puertos designados en el puente raíz de su región. De este modo, se conservan los puertos designados en el puente raíz de su región.

Nota: Seleccione cuidadosamente la raíz y una raíz de respaldo para cada instancia.

Colocación del puente raíz en el CIST en el switch Catalyst - CLI

```
Catalyst(config)# spanning-tree mst [instance-id] root {primary | secondary} [diámetro dia  
[hello-time hello-time]]
```

```
Catalyst(config)# spanning-tree mst 1 root primario 7
```

Resolución de problemas - Catalyst

El siguiente comando devolverá El siguiente comando devolverá cualquier puerto que haya sido marcado como inconsistente. Pero también tenga en cuenta que el comando no está disponible en los switches SMB.

```
Catalyst# show spanning-tree inconsistentports
```

Colocación del puente raíz en el CIST en el switch SMB - CLI

```
SMBswitch(config)# interface [interface-id]  
SMBswitch(config-if)# spanning-tree guard root
```

```
SMBswitch(config)# interfaz gil/1/1  
SMBswitch(config-if)# raíz de protección del árbol de expansión
```

Colocación del puente raíz en el CIST en el switch para PYMES - GUI

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Spanning Tree > STP Interface Settings**.

Paso 2. Elija una **interfaz** de la lista desplegable *Tipo de interfaz*.

Paso 3. Haga clic en **Ir** para mostrar una lista de puertos o LAG en la interfaz.

Paso 4. Haga clic en el **botón de opción** del puerto o **LAG** que desea modificar y haga clic en

Editar. Aparece la ventana Edit STP Interface Setting (Editar configuración de interfaz STP).

Paso 5. Haga clic en el **botón de opción** que corresponde a la interfaz deseada en el campo Interfaz.

- Puerto: en la lista desplegable Puerto, elija el puerto que desea configurar. Esto sólo afectará al puerto único elegido.
- LAG: en la lista desplegable LAG, elija el LAG que desea configurar. Esto afectará al grupo de puertos definido en la configuración LAG.

Paso 6. Asegúrese de que el STP esté marcado **Enable** en el *campo STP* para habilitar el STP en la interfaz.

Paso 7. Marque **Enable** en el campo *Root Guard* para habilitar Root Guard en la interfaz. Esta opción proporciona una forma de aplicar la ubicación del puente raíz en la red. La protección de raíz se utiliza para evitar que un nuevo dispositivo conectado tome el control como puente raíz.

Verificación de la migración - ¿Está esto en marcha?

En este momento, la implementación y la red de MSTP deben continuar. Para la multitud de confianza pero verificación, puede verificar el estado de MSTP mediante la realización de una captura de tramas. A continuación, compare los resultados con la documentación esperada.

Después de realizar una captura de paquetes a través de Wireshark, verá *Mrecords* que contienen el identificador de la instancia. A continuación se muestra una captura de pantalla de *Mrecord*, antes de la expansión para obtener más detalles.

```
▼ Spanning Tree Protocol
  Protocol Identifier: Spanning Tree Protocol (0x0000)
  Protocol Version Identifier: Multiple Spanning Tree (3)
  BPDU Type: Rapid/Multiple Spanning Tree (0x02)
  ▶ BPDU flags: 0x7c, Agreement, Forwarding, Learning, Port Role: Designated
  ▶ Root Identifier: 24576 / 0 / 24:e9:b3:78:fe:80
  Root Path Cost: 0
  ▶ Bridge Identifier: 24576 / 0 / 24:e9:b3:78:fe:80
  Port identifier: 0x8018
  Message Age: 0
  Max Age: 20
  Hello Time: 2
  Forward Delay: 15
  Version 1 Length: 0
  Version 3 Length: 96
  ▼ MST Extension
    MST Config ID format selector: 0
    MST Config name: Cisco
    MST Config revision: 1
    MST Config digest: 2a5477095c475f337a69c797b32cd60a
    CIST Internal Root Path Cost: 0
    ▶ CIST Bridge Identifier: 24576 / 0 / 24:e9:b3:78:fe:80
    CIST Remaining hops: 20
    ▶ MSTID 1, Regional Root Identifier 24576 / 24:e9:b3:78:fe:80
    ▶ MSTID 2, Regional Root Identifier 24576 / 24:e9:b3:79:06:00
```

MRecords

Expandir el *Mrecord* Permite ver datos más granulares sobre MSTP. Incluidos:

- Función de puerto

- ID de MST
- Raíz regional
- Costo de trayecto interno
- Prioridad del identificador del puente
- Prioridad del identificador de puerto
- Saltos restantes

```

▼ MSTID 1, Regional Root Identifier 24576 / 24:e9:b3:78:fe:80
  ► MSTI flags: 0x7c, Agreement, Forwarding, Learning, Port Role: Designated
    0110 .... = Priority: 0x6
    .... 0000 0000 0001 = MSTID: 1
    Regional Root: Cisco_78:fe:80 (24:e9:b3:78:fe:80)
    Internal root path cost: 0
    Bridge Identifier Priority: 6
    Port identifier priority: 8
    Remaining hops: 20
▼ MSTID 2, Regional Root Identifier 24576 / 24:e9:b3:79:06:00
  ► MSTI flags: 0x78, Agreement, Forwarding, Learning, Port Role: Root
    0110 .... = Priority: 0x6
    .... 0000 0000 0010 = MSTID: 2
    Regional Root: Cisco_79:06:00 (24:e9:b3:79:06:00)
    Internal root path cost: 20000
    Bridge Identifier Priority: 8
    Port identifier priority: 8
    Remaining hops: 20

```

Comandos de verificación rápida - SMB CLI

Si desea verificar desde la línea de comandos, intente estos comandos:

```
SMBswitch# show spanning-tree mst-configuration
```

```
SMBswitch(config)# spanning-tree mst-configuration
```

```
SMBswitch(config-mst)# show pending
```

Configuración MST pendiente

Nombre [region1]

Revisión 1

Instancias configuradas 2

Instancia Vlan Asignada

- -

0 1-9,21-4094

1 10-20

-

```
SMBswitch# show spanning-tree mst-configuration
```

Nombre []

Revisión 0

Vlan de instancia asignada

- -

0 1-4094

-

Nota: La versión de Catalyst del comando show excluye el - entre la configuración y el mst.
EX:"show spanning-tree mst configuration"

Qué debe saber sobre PVST+ y MSTP que viven en la misma red

Si necesita continuar con el soporte para los switches heredados que ejecutan PVST+, maneje esto puerto por puerto. Si uno de estos switches se ejecuta como troncal VLAN, asegúrese de que el switch MSTP sea la raíz de todas las VLAN asignadas al tronco. Además, MSTP intenta decodificar PVST+ BPDU, pero esta simulación es imperfecta. Lo que nos obliga a profundizar

en la idea de los puertos fronterizos.

El rol y el estado de un puerto de límite MSTP lo determina el *árbol de expansión interno* que interactúa con la topología exterior. Esto significa que si un puerto está en modo de bloqueo en el *IST*, entonces está bloqueando en todas las instancias de MSTP. Este efecto se adentra en cascada en la implementación de PVST+, afectando la función de VLAN. Lo mismo sucede si el puerto reenvía, aprende, etc. Como puede imaginar, esto puede convertirse en un problema. Esto puede resultar en un problema intratable mientras que un puerto que debería estar reenviando para una VLAN, en cambio está bloqueando, debido a las necesidades de otra VLAN. La simulación PVST+ aprovecha la información del *IST* para crear BPDU por VLAN. Esto da como resultado una "ilusión" en toda la red de que la región MSTP aparece como un único switch para todas las VLAN. Similar a la manera en que los switches son capaces de *apilarse*, lo que no es mitad malo. Lo que es malo, desde la posición del puerto de frontera, es que crea la necesidad de enviar BPDU individuales para cada VLAN simulada. Cualquier inconsistencia entre las BPDU puede destruir toda la simulación en errores. Sólo la recepción de BPDU consistentes permitirá que la simulación se detenga a sí misma.

Para concluir, toda esta situación es la razón por la que las BPDU recibidas en el puerto de límite deben ser idénticas. [Para obtener más información sobre este tema, consulte este subproceso de la comunidad.](#)

¿Hay algo que saber, si mi hardware de red...¿no es completamente Cisco?

MSTP es compatible con versiones anteriores. Siempre y cuando su hardware que no sea de Cisco admita el árbol de expansión rápido, debería estar en lo correcto. Si tiene problemas, [consulte con nuestra comunidad de switching.](#)

Conclusión

Gracias por leer esta guía, con estas prácticas recomendadas debe configurarse para mejorar el rendimiento de su red de capa 2.

Cabe destacar que el árbol de extensión puede no resultarle emocionante, pero las ventajas de compartir la carga hacen que merezca la pena el esfuerzo por mantener su red eficiente. Al creador del árbol de expansión, Radia Perlman, le encanta tanto como una madre pudo. Incluso escribió un [al respecto.](#)