

Resolución de problemas del switch Catalyst VMPS

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Membresía de DVLAN del Troubleshooting](#)

[Antes de que usted resuelva problemas el Membresía de DVLAN](#)

[Conectividad del Troubleshooting entre el PC y el Switch del cliente de VMPS](#)

[Problemas de conectividad del Troubleshooting entre el cliente de VMPS y el VMPS](#)

[Resuelva problemas el archivo de base de datos VMPS](#)

[Resuelva problemas descarga del archivo de base de datos VMPS](#)

[Resuelva problemas a los clientes de VMPS 2900XL/3500XL/2950/3550](#)

[Advertencias VMPS conocidas](#)

[Información a recolectar antes de que usted entre en contacto el Soporte técnico de Cisco](#)

[Información Relacionada](#)

[Introducción](#)

Con el Servidor de políticas de administración de VLAN (VMPS), un administrador de un switch Catalyst puede asignar dinámicamente un dispositivo de red a una VLAN específica. Esta tecnología resulta útil en lugares con gran cantidad de usuarios móviles. Este documento trata de cómo resolver problemas de registro del host en VMPS de un switch Catalyst. El registro del host hace referencia a la capacidad de asignar una VLAN en función de la dirección Ethernet MAC de un PC. Este documento trata sobre el nivel mínimo de software necesario para ejecutar tanto VMPS como el cliente VMPS y ofrece sugerencias sobre cómo resolver problemas de las diversas etapas y componentes de una asignación de VLAN Dinámica (DVLAN).

Nota: El VMPS del switch Catalyst proporciona solamente el registro del host. Para asignar un VLAN con la autenticación de NT (también conocida como inscripción de usuario) utilice el [Cisco Secure User Registration Tool](#).

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

Componentes Utilizados

Esta tabla enumera los requisitos mínimos de software de soportar el VMPS en los diversos Productos del Switch del Cisco Catalyst:

Producto	Soporte VMPS	Soporte VMPS de cliente
Catalyst 4000 Family (Catalyst OS)	Sí, 7.2(x) y posterior	Sí, todas las versiones de software
Catalyst 4000/4500 (Cisco IOS Software)	Soportado o no actualmente	Sí, 12.1(13)EW y posterior
Catalyst 2900XL/3500XL	No soportados	Sí, 11.2(8)SA4 y posterior, edición del software para empresas solamente
Catalyst 2950/2955/3550	No soportados	Sí, todas las versiones de software
Catalyst 2948G-L3/4908G-L3	No soportados	No soportados
Familia Catalyst 5000/5500	Sí, 2.3.x y posterior	Sí, 2.3.x y posterior
Familia del Catalyst 6000/6500 (Catalyst OS)	Sí, 6.1(x) y posterior	Sí, todas las versiones de software
Familia del Catalyst 6000/6500 (Cisco IOS Software)	Soportado o no actualmente	Soportado no actualmente

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

Resuelva problemas el Membresía de DVLAN

El Protocolo de consulta de VLAN (VQP) es el transporte principal para la información de VMPS. El VQP utiliza el Protocolo de Datagrama de Usuario (UDP) puerto 1589. Este ejemplo ilustra los

pasos importantes en el proceso del Membresía de DVLAN, y muestra cómo asignan un cliente dinámicamente un VLA N en base de la dirección MAC:

1. El PC envía una trama al Switch.
2. El cliente de VMPS aprende la dirección MAC PC en el puerto dinámico.
3. El cliente de VMPS envía una petición VQP al VMPS. La petición contiene la dirección IP del cliente de VMPS, la dirección MAC PC, el número del puerto de PC, y el dominio VTP.
4. Los VMPS parsis el archivo de base de datos para la asignación VLAN PC.
5. El VMPS envía una respuesta VQP al cliente de VMPS.
6. Si la respuesta VQP contiene una asignación VLAN, el cliente de VMPS la asigna al VLA N. Si no, el cliente niega acceso de PC.

Usted puede clasificar la mayoría de los problemas que usted encuentre en estas tres categorías:

- Problemas de conectividad entre el PC y el cliente de VMPS. Vea [antes de resolver problemas el Membresía de DVLAN](#) y de [resolver problemas la Conectividad entre el PC y las secciones del Switch del cliente de VMPS de](#) este documento.
- Problemas de conectividad entre el cliente de VMPS y el VMPS. Vea que la [Conectividad del troubleshooting entre el cliente de VMPS y el VMPS](#) y el [troubleshooting que las secciones del archivo de la base de datos VMPS de](#) este documentan.
- Problemas de la configuración de archivos de la base de datos VMPS. Vea el [troubleshooting la sección del archivo de la base de datos VMPS de](#) este documento.

[Antes de que usted resuelva problemas el Membresía de DVLAN](#)

Antes de que usted resuelva problemas los problemas del Membresía de DVLAN en un cliente de VMPS que funcione con el Catalyst OS (CatOS), aumente el nivel de registro DVLAN en el cliente de VMPS del nivel de registro 2 al nivel de registro 7 (debugging). Entonces, publique el **comando set logging level dvlan 7 default**.

Nota: En algunas versiones de CatOS, cuando usted aumenta el nivel de registro DVLAN, un error puede ocurrir, que estado que esto es un recurso inválido. Este error es un resultado del Id. de bug Cisco [CSCdu19163 \(clientes registrados solamente\)](#), y este problema se resuelve en los Cisco IOS Software Release 5.5(8), 6.3(1), y posterior.

Usted debe habilitar este comando en los clientes de VMPS cuando usted resuelve problemas porque este comando proporciona la información vital sobre el error del Membresía de DVLAN.

Después de que usted complete el troubleshooting y resuelva el problema, usted puede reducir el nivel de registro DVLAN del nivel de registro 7 al problema del nivel de registro 2. el **comando set logging level dvlan 2 default**.

En los switches CatOS, usted puede realizar el debugging adicional si usted publica el **comando set trace dynvlan 6** dirigido por un ingeniero de soporte técnico. Habilite este comando antes de que usted enchufe o accione para arriba el PC con los problemas de la asignación VLAN. Espere cerca de un minuto antes de que usted inhabilita el comando. Para inhabilitar el comando, publique el **comando set trace dynvlan 0** en el enable mode.

Precaución: Habilite este comando con cautela. La salida de los debugs puede hacer el Switch causar un crash, si varios PC salen y se unen a de los puertos dinámicos en el mismo Switch. Usted debe inhabilitar el registro de la consola antes de que usted habilite este comando.

Conectividad del Troubleshooting entre el PC y el Switch del cliente de VMPS

Los problemas de conectividad entre el PC y el cliente de VMPS pueden hacer el Membresía de DVLAN fallar si el Switch del cliente de VMPS no puede obtener la dirección MAC del PC. En este caso, el puerto permanece en el estado “inactivo” con una asignación VLAN del `dyn`, tal y como se muestra en de este ejemplo:

```
vmpls_client> (enable) show port 3/2
```

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
3/2		inactive	dyn-	normal	a-half	a-10	10/100BaseTX

Cuando una confirmación reconfirmación VMPS ocurre en el Switch del cliente de VMPS y el Switch no puede obtener la dirección MAC de ningún PC en ningún puerto dinámico, después este mensaje aparece:

```
vmpls_client> (enable) show port 3/2
```

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
3/2		inactive	dyn-	normal	a-half	a-10	10/100BaseTX

La confirmación reconfirmación VMPS ocurre cuando el cliente de VMPS pide el VMPS si las asignaciones de puerto dinámico están correctas y si las direcciones MAC correctas se han asignado a los puertos correctos. Por abandono, esta reconfirmación ocurre sobre cada 60 minutos. Ejecute el comando `show vmpls` en el cliente VMPS para determinar el tiempo de reconfirmación de VMPS.

Si usted está seguro que hay por lo menos un PC conectado con un puerto dinámico, realice estos pasos:

1. Desconecte el PC del Switch.
2. Publique un **comando ping del PC** a dondequiera.
3. Publique el **comando reconfirm vmpls** en el cliente de VMPS de conexión.

El cliente de VMPS intenta confirmar con el VMPS que el direccionamiento del PC se debe asignar a ese puerto. Si la dirección MAC no puede ser reconfirmada, este mensaje aparece:

```
vmpls_client> (enable) show port 3/2
```

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
3/2		inactive	dyn-	normal	a-half	a-10	10/100BaseTX

El problema puede ser un problema con la base de datos VMPS (véase el [troubleshooting la sección del archivo de la base de datos VMPS de](#) este documento) o con la comunicación entre el cliente de VMPS y el VMPS (véase la [Conectividad del troubleshooting entre el cliente de VMPS y la](#) sección [VMPS de](#) este documento).

Si el Switch del cliente de VMPS continúa estado que no hay host conectado con el puerto dinámico, y los abortos de la reconfirmación, resuelva problemas el problema como problema de conectividad de la Capa física entre un cliente de VMPS y un PC. Para más información, refiera a la [sección de Troubleshooting de la Capa física de puerto del switch del troubleshooting e interconecte los problemas.](#)

Resuelva problemas los problemas de conectividad entre el cliente de VMPS y el VMPS

Cuando una pérdida de conectividad ocurre entre un cliente de VMPS y un VMPS, la confirmación reconfirmación VMPS puede fallar y presentar el mensaje de error `DVLAN-2-MACNOTRECONFIRMED`. El puerto pierde la asignación de DVLAN, como en este ejemplo:

```
vmpls_client> (enable) show port 3/2
```

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
3/2		inactive	dyn-	normal	a-half	a-10	10/100BaseTX

La confirmación reconfirmación VMPS ocurre cuando el cliente de VMPS pide el VMPS si las asignaciones de puerto dinámico están correctas y si las direcciones MAC correctas se han asignado a los puertos derechos. Por abandono, este control ocurre sobre cada 60 minutos. Publique un **comando show vmpls** en el cliente de VMPS de determinar el tiempo de la confirmación reconfirmación VMPS.

Complete estos pasos para resolver problemas los problemas de conectividad entre un cliente de VMPS y un VMPS:

1. Haga ping con VMPS desde el cliente VMPS. Si el ping falla, resuelva problemas el problema como problema general de la conectividad del switch o como problema de ruteo general. Para más información, consulte [Configuración del ruteo de InterVLAN y de la conexión troncal de ISL/802.1Q en un switch Catalyst 2900XL/3500XL/2950 mediante un router externo](#).
2. Si el **comando ping** es acertado entre el cliente de VMPS y el VMPS, asegúrese de que no haya dispositivo — entre el cliente de VMPS y el trayecto de red VMPS — ese bloquee el puerto 1589 UDP.
3. Si la Conectividad entre el cliente de VMPS y el VMPS es intermitente (un ciertos datos consiguen perdidos a lo largo del camino), usted puede intentar aumentar el intervalo entre reintentos VMPS en el cliente de VMPS, como solución alternativa. Publique el **comando set vmpls server retry**. Por abandono, el cliente de VMPS intenta tres veces. En un entorno con la Conectividad intermitente, cuando usted aumenta el intervalo entre reintentos VMPS, usted da a cliente más oportunidades de conectar con el VMPS antes de que el cliente abandone y la calidad de miembro de VLAN falla.

[Resuelva problemas el archivo de base de datos VMPS](#)

El archivo de base de datos VMPS define todos los parámetros que registro del host del control en el VMPS del switch Catalyst. Usted debe crear manualmente el archivo con un editor de textos. Éstos son los cuatro componentes primarios de la base de datos VMPS:

- Grupo de puertos — Una colección de puertos encontrados en el diverso Switches.
- Grupo VLAN — Una colección de VLA N que se pueden asociar a un grupo de puertos.
- Política de puerto — Asocia a un grupo de puertos a un grupo VLAN o a un nombre del VLA N.
- Dirección MAC a la tabla de asociación del VLA N — Especifica a qué VLA N se asigna una dirección MAC. **Nota:** Usted puede asignar una dirección MAC solamente a un VLA N. Si tiene una dirección MAC asociada con dos VLAN diferentes, sólo se usa la primera que se enumera. **Nota:** El caso práctico siguiente ilustra cómo el archivo de base de datos VMPS funciona y le ayuda a resolver problemas cualquier problema del error de la base de datos VMPS.

Descripción del caso práctico

La compañía XYZ tiene estas tres áreas:

- El área 1 contiene los cuartos y los recursos del entrenamiento.
- El área 2 está para los ejecutivos y los ejecutivos de ventas.
- El área 3 está para los ingenieros.

Tres VLA N llamanon “executive_vlan,” “sales_vlan,” y “eng_vlan” se crean. Los ejecutivos se deben poner en el VLA N executive_vlan, si están en su oficina o en el cuarto del entrenamiento. Todos los PC del Representante representante de ventas se asignan al sales_vlan, y todos los PC de los ingenieros se asignan al eng_vlan.

Éste es un ejemplo del esquema del diseño de la compañía XYZ:

Switch	Área	Configuración
A	Área de entrenamiento	Conceden el acceso a todos los puertos y se asignan los ejecutivos, los ejecutivos de ventas, y los ingenieros a sus VLAN respectivos.
B	Ventas /área ejecutiva	Solamente los PC ejecutivos se conceden el acceso al puerto 2/1-5; el ejecutivo PC se asigna a executive_vlan. Solamente los ejecutivos de ventas PC tienen acceso al puerto 2/10-15; asignan los ejecutivos de ventas PC a sales_vlan. El acceso a otros puertos en el Switch se niega a los ejecutivos, a los ejecutivos de ventas, y a los ingenieros.
C	Dirigir el área	Solamente dirigiendo los PC se conceden el acceso al Switch; dirigiendo los PC se asignan a eng_vlan.

Nombre de dominio VMPS y Nombre de dominio VTP

El Domain Name VMPS y el Domain Name del VLAN Trunk Protocol (VTP) deben hacer juego. El dominio VMPS distingue entre mayúsculas y minúsculas. Por ejemplo, si el Domain Name VTP es “XYZ_company”, el Domain Name VMPS debe ser “XYZ_company” y no “xyz_company.”

Política de puerto VMPS

Tres políticas de puerto serán creadas: el primer para los ejecutivos, el segundo para los ejecutivos de ventas, y el tercero para los ingenieros.

Una vez más los nombres del VLA N usados para crear las políticas de puerto VMPS son con diferenciación entre mayúsculas y minúsculas y deben hacer juego el nombre del VLA N en la base de datos de VLAN. Como regla general, Cisco recomienda que usted utiliza la minúscula para nombrar todos los VLA N y dominios VTP.

Los estados ejecutivos de la política de puerto que un ejecutivo PC conectó con el puerto 2/1-5 en el switch B (192.168.2.2) o cualquier puerto en el Switch A (192.168.2.1) se asigna a `executive_vlan`.

Los estados de la política de puerto de las ventas que los ejecutivos de ventas PC conectaron con el puerto 2/11-15 en el switch B (192.168.2.2) o cualquier puerto en el Switch A (192.168.2.1) se asigna a `sales_vlan`.

Los estados de la política de puerto de la ingeniería que asignan un ingeniero PC conectado con cualquier puerto en el Switch A (192.168.2.1) o el C del Switch (192.168.2.3) a `eng_vlan`.

Niegan se apagan el resto de los usuarios que intentan conectar con los puertos dinámicos el acceso y el puerto. Un mensaje de Syslog informa al administrador el cierre de puerto, y la acción apropiada se toma después de eso.

Este archivo de configuración de VMPS de la muestra para la compañía XYZ muestra el archivo de base de datos VMPS resultante:

```
!--- VMPS domain name must be the same as the VTP domain of the network. !--- This value is case sensitive. If the VTP domain is TestVmps, the VMPS !--- domain must also be TestVmps. vmps domain xyz_company ! !--- If the VMPS cannot assign the host a VLAN, shut down the port. If the !--- VMPS mode is "open," a log message, which states that access is denied !--- is produced and the port becomes inactive. vmps mode secure ! !--- No fallback VLAN is configured for the XYZ network, so it is commented out. !--- A fallback VLAN is assigned to a PC whose MAC address is not present in the !--- database. The fallback VLAN is usually a VLAN where a user cannot access !--- sensitive network resources. !! vmps fallback nonsecure_vlan ! !--- List of MAC addresses that will be assigned to a VLAN. !--- The VLAN-name matches the names given to VLANs on the VMPS. !--- VLAN names are case sensitive, as is the VMPS domain name. ! !--- MAC address format must be xxxx.xxxx.xxxx . Any other format will not work. !vmps-mac-addr address 0000.0000.0001 vlan-name eng_vlan address 0000.0000.0002 vlan-name eng_vlan address 0000.0000.0003 vlan-name sales_vlan address 0000.0000.0004 vlan-name sales_vlan address 0000.0000.0005 vlan-name executive_vlan address 0000.0000.0006 vlan-name executive_vlan !!!!!!!!!!!!!!! Executive policy !!!!!!!!!!!!!!! !--- This port policy states that the VMPS checks the MAC address of the !--- PC plugged in any port in Switch A (192.168.2.1) or port 2/1-5 in !--- Switch B (192.168.2.2) against the MAC addresses associated to the !--- executive_vlan in the vmps-mac-addr database. ! !--- When you create a port group, a range command such as !--- device x.x.x.x port 2/1-5 is not allowed. This will produce !--- a parse error when the VMPS database downloads.
```

```
vmps-vlan-group executive
vlan-name executive_vlan
!
vmps-port-group executive_ports
device 192.168.2.1 all-ports
device 192.168.2.2 port 2/1
device 192.168.2.2 port 2/2
device 192.168.2.2 port 2/3
device 192.168.2.2 port 2/4
device 192.168.2.2 port 2/5
!
vmps-port-policies vlan-group executive
port-group executive_ports
!
!!!!!!!!!!!!!! Sales policy !!!!!!!!!!!!!!!
!--- This port policy states that the VMPS checks the MAC address !--- of the PC plugged in any port in Switch A (192.168.2.1) or port !--- 2/10-15 in Switch B (192.168.2.2) against the MAC addresses associated !--- to the sales_vlan in the vmps-mac-addr database. ! !--- Notice that you can bind a port group to a VLAN name instead of a !--- VLAN group. A VLAN group allows a port group to be bound to multiple !--- VLANs. In this case, the ports defined in the port group
```

```

sales_port can use !--- the MAC addresses defined in the sales_vlan. vmps-vlan-group sales vlan-
name sales_vlan ! vmps-port-group sales_ports device 192.168.2.1 all-ports device 192.168.2.2
port 2/10 device 192.168.2.2 port 2/11 device 192.168.2.2 port 2/12 device 192.168.2.2 port 2/13
device 192.168.2.2 port 2/14 device 192.168.2.2 port 2/15 ! vmps-port-policies vlan-name
sales_vlan
port-group sales_ports
!
!!!!!!!!!!!!!! Engineer policy !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- This port policy states that the VMPS checks the MAC address of !--- the PC plugged in any
port in Switch A (192.168.2.1) or Switch C !--- (192.168.2.3) against the MAC addresses
associated to the eng_vlan !--- in the vmps-mac-addr database. ! vmps-vlan-group engineering
vlan-name eng_vlan ! vmps-port-group eng_ports device 192.168.2.1 all-ports device 192.168.2.3
all-ports ! vmps-port-policies vlan-group engineering
port-group eng_ports
!

```

[Resuelva problemas descarga del archivo de base de datos VMPS](#)

Para que el VMPS funcione correctamente, usted debe descargar la base de datos y el archivo de configuración de un (RCP) del Remote Copy Protocol o el servidor del Trivial File Transfer Protocol (TFTP) al Switch VMPS. Este proceso falla en estos escenarios:

- **Cuando el archivo de base de datos VMPS no existe ni se nombra incorrectamente en el RCP o el servidor TFTP.** Si el archivo de base de datos no existe ni hace juego el campo del archivo de base de datos en la salida del **comando show vmps** del Switch VMPS, el Switch VMPS produce este error:

```

!--- VMPS domain name must be the same as the VTP domain of the network. !--- This value is
case sensitive. If the VTP domain is TestVmps, the VMPS !--- domain must also be TestVmps.
vmps domain xyz_company ! !--- If the VMPS cannot assign the host a VLAN, shut down the
port. If the !--- VMPS mode is "open," a log message, which states that access is denied !--
- is produced and the port becomes inactive. vmps mode secure ! !--- No fallback VLAN is
configured for the XYZ network, so it is commented out. !--- A fallback VLAN is assigned to
a PC whose MAC address is not present in the !--- database. The fallback VLAN is usually a
VLAN where a user cannot access !--- sensitive network resources. !! vmps fallback
nonsecure_vlan ! !--- List of MAC addresses that will be assigned to a VLAN. !--- The VLAN-
name matches the names given to VLANs on the VMPS. !--- VLAN names are case sensitive, as is
the VMPS domain name. ! !--- MAC address format must be xxxx.xxxx.xxxx . Any other format
will not work. !vmps-mac-addr address 0000.0000.0001 vlan-name eng_vlan address
0000.0000.0002 vlan-name eng_vlan address 0000.0000.0003 vlan-name sales_vlan address
0000.0000.0004 vlan-name sales_vlan address 0000.0000.0005 vlan-name executive_vlan address
0000.0000.0006 vlan-name executive_vlan ! !!!!!!!!!!!!!!! Executive policy
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- This port policy states that the VMPS checks the MAC
address of the !--- PC plugged in any port in Switch A (192.168.2.1) or port 2/1-5 in !---
Switch B (192.168.2.2) against the MAC addresses associated to the !--- executive_vlan in
the vmps-mac-addr database. ! !--- When you create a port group, a range command such as !-
- device x.x.x.x port 2/1-5 is not allowed. This will produce !--- a parse error when the
VMPS database downloads.

```

```

vmps-vlan-group executive
vlan-name executive_vlan
!
vmps-port-group executive_ports
device 192.168.2.1 all-ports
device 192.168.2.2 port 2/1
device 192.168.2.2 port 2/2
device 192.168.2.2 port 2/3
device 192.168.2.2 port 2/4
device 192.168.2.2 port 2/5
!
vmps-port-policies vlan-group executive
port-group executive_ports

```



```

!
!!!!!!!!!!!!!! Sales policy !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- This port policy states that the VMPS checks the MAC address !--- of the PC plugged in
any port in Switch A (192.168.2.1) or port !--- 2/10-15 in Switch B (192.168.2.2) against
the MAC addresses associated !--- to the sales_vlan in the vmps-mac-addr database. ! !---
Notice that you can bind a port group to a VLAN name instead of a !--- VLAN group. A VLAN
group allows a port group to be bound to multiple !--- VLANs. In this case, the ports
defined in the port group sales_port can use !--- the MAC addresses defined in the
sales_vlan. vmps-vlan-group sales vlan-name sales_vlan ! vmps-port-group sales_ports device
192.168.2.1 all-ports device 192.168.2.2 port 2/10 device 192.168.2.2 port 2/11 device
192.168.2.2 port 2/12 device 192.168.2.2 port 2/13 device 192.168.2.2 port 2/14 device
192.168.2.2 port 2/15 ! vmps-port-policies vlan-name sales_vlan
port-group sales_ports
!
!!!!!!!!!!!!!! Engineer policy !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- This port policy states that the VMPS checks the MAC address of !--- the PC plugged in
any port in Switch A (192.168.2.1) or Switch C !--- (192.168.2.3) against the MAC addresses
associated to the eng_vlan !--- in the vmps-mac-addr database. ! vmps-vlan-group
engineering vlan-name eng_vlan ! vmps-port-group eng_ports device 192.168.2.1 all-ports
device 192.168.2.3 all-ports ! vmps-port-policies vlan-group engineering
port-group eng_ports
!

```

- Cuando el Switch VMPS no puede entrar en contacto el RCP o al servidor TFTP. Si el Switch VMPS no puede conectar con el RCP o el servidor TFTP, el Switch VMPS produce este error:

```

!--- VMPS domain name must be the same as the VTP domain of the network. !--- This value is
case sensitive. If the VTP domain is TestVmps, the VMPS !--- domain must also be TestVmps.
vmps domain xyz_company ! !--- If the VMPS cannot assign the host a VLAN, shut down the
port. If the !--- VMPS mode is "open," a log message, which states that access is denied !--
- is produced and the port becomes inactive. vmps mode secure ! !--- No fallback VLAN is
configured for the XYZ network, so it is commented out. !--- A fallback VLAN is assigned to
a PC whose MAC address is not present in the !--- database. The fallback VLAN is usually a
VLAN where a user cannot access !--- sensitive network resources. !! vmps fallback
nonsecure_vlan ! !--- List of MAC addresses that will be assigned to a VLAN. !--- The VLAN-
name matches the names given to VLANs on the VMPS. !--- VLAN names are case sensitive, as is
the VMPS domain name. ! !--- MAC address format must be xxxx.xxxx.xxxx . Any other format
will not work. !vmps-mac-addr address 0000.0000.0001 vlan-name eng_vlan address
0000.0000.0002 vlan-name eng_vlan address 0000.0000.0003 vlan-name sales_vlan address
0000.0000.0004 vlan-name sales_vlan address 0000.0000.0005 vlan-name executive_vlan address
0000.0000.0006 vlan-name executive_vlan ! !!!!!!!!!!!!!!! Executive policy
!!!!!!!!!!!!!! !--- This port policy states that the VMPS checks the MAC
address of the !--- PC plugged in any port in Switch A (192.168.2.1) or port 2/1-5 in !---
Switch B (192.168.2.2) against the MAC addresses associated to the !--- executive_vlan in
the vmps-mac-addr database. ! !--- When you create a port group, a range command such as !-
-- device x.x.x.x port 2/1-5 is not allowed. This will produce !--- a parse error when the
VMPS database downloads.

```

```

vmps-vlan-group executive
vlan-name executive_vlan
!
vmps-port-group executive_ports
device 192.168.2.1 all-ports
device 192.168.2.2 port 2/1
device 192.168.2.2 port 2/2
device 192.168.2.2 port 2/3
device 192.168.2.2 port 2/4
device 192.168.2.2 port 2/5
!
vmps-port-policies vlan-group executive
port-group executive_ports
!

```

```

!!!!!!!!!!!!!! Sales policy !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- This port policy states that the VMPS checks the MAC address !--- of the PC plugged in
any port in Switch A (192.168.2.1) or port !--- 2/10-15 in Switch B (192.168.2.2) against

```

```

the MAC addresses associated !--- to the sales_vlan in the vmmps-mac-addr database. ! !---
Notice that you can bind a port group to a VLAN name instead of a !--- VLAN group. A VLAN
group allows a port group to be bound to multiple !--- VLANs. In this case, the ports
defined in the port group sales_port can use !--- the MAC addresses defined in the
sales_vlan. vmmps-vlan-group sales_vlan-name sales_vlan ! vmmps-port-group sales_ports device
192.168.2.1 all-ports device 192.168.2.2 port 2/10 device 192.168.2.2 port 2/11 device
192.168.2.2 port 2/12 device 192.168.2.2 port 2/13 device 192.168.2.2 port 2/14 device
192.168.2.2 port 2/15 ! vmmps-port-policies vlan-name sales_vlan
port-group sales_ports
!
!!!!!!!!!!!!!! Engineer policy !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- This port policy states that the VMPS checks the MAC address of !--- the PC plugged in
any port in Switch A (192.168.2.1) or Switch C !--- (192.168.2.3) against the MAC addresses
associated to the eng_vlan !--- in the vmmps-mac-addr database. ! vmmps-vlan-group
engineering vlan-name eng_vlan ! vmmps-port-group eng_ports device 192.168.2.1 all-ports
device 192.168.2.3 all-ports ! vmmps-port-policies vlan-group engineering
port-group eng_ports

```

!Tenga en cuenta que éste es el mismo error que el que se produce si el switch VMPS puede contactar al servidor RCP o TFTP, pero el archivo de la base de datos no existe o tiene asignado un nombre incorrecto. En este caso, usted debe verificar la conectividad de red entre el RCP o el servidor TFTP y el Switch VMPS. Si la conectividad de red existe entre el VMPS y el cliente de VMPS, verifique si el puerto RCP o TFTP del servidor esté abierto y listo para recibir las conexiones.

- **Cuando el archivo de base de datos contiene los Errores de configuración.** Si un error de la configuración de la base de datos se detecta durante la descarga, el Switch VMPS produce este error:

```

!--- VMPS domain name must be the same as the VTP domain of the network. !--- This value is
case sensitive. If the VTP domain is TestVmmps, the VMPS !--- domain must also be TestVmmps.
vmmps domain xyz_company ! !--- If the VMPS cannot assign the host a VLAN, shut down the
port. If the !--- VMPS mode is "open," a log message, which states that access is denied !---
is produced and the port becomes inactive. vmmps mode secure ! !--- No fallback VLAN is
configured for the XYZ network, so it is commented out. !--- A fallback VLAN is assigned to
a PC whose MAC address is not present in the !--- database. The fallback VLAN is usually a
VLAN where a user cannot access !--- sensitive network resources. !! vmmps fallback
nonsecure_vlan ! !--- List of MAC addresses that will be assigned to a VLAN. !--- The VLAN-
name matches the names given to VLANs on the VMPS. !--- VLAN names are case sensitive, as is
the VMPS domain name. ! !--- MAC address format must be xxxx.xxxx.xxxx . Any other format
will not work. !vmmps-mac-addr address 0000.0000.0001 vlan-name eng_vlan address
0000.0000.0002 vlan-name eng_vlan address 0000.0000.0003 vlan-name sales_vlan address
0000.0000.0004 vlan-name sales_vlan address 0000.0000.0005 vlan-name executive_vlan address
0000.0000.0006 vlan-name executive_vlan ! !!!!!!!!!!!!!!! Executive policy
!!!!!!!!!!!!!! !--- This port policy states that the VMPS checks the MAC
address of the !--- PC plugged in any port in Switch A (192.168.2.1) or port 2/1-5 in !---
Switch B (192.168.2.2) against the MAC addresses associated to the !--- executive_vlan in
the vmmps-mac-addr database. ! !--- When you create a port group, a range command such as !-
-- device x.x.x.x port 2/1-5 is not allowed. This will produce !--- a parse error when the
VMPS database downloads.

```

```

vmmps-vlan-group executive
vlan-name executive_vlan
!
vmmps-port-group executive_ports
device 192.168.2.1 all-ports
device 192.168.2.2 port 2/1
device 192.168.2.2 port 2/2
device 192.168.2.2 port 2/3
device 192.168.2.2 port 2/4
device 192.168.2.2 port 2/5
!
vmmps-port-policies vlan-group executive
port-group executive_ports

```

```

!
!!!!!!!!!!!!!! Sales policy !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- This port policy states that the VMPS checks the MAC address !--- of the PC plugged in
any port in Switch A (192.168.2.1) or port !--- 2/10-15 in Switch B (192.168.2.2) against
the MAC addresses associated !--- to the sales_vlan in the vmps-mac-addr database. ! !---
Notice that you can bind a port group to a VLAN name instead of a !--- VLAN group. A VLAN
group allows a port group to be bound to multiple !--- VLANs. In this case, the ports
defined in the port group sales_port can use !--- the MAC addresses defined in the
sales_vlan. vmps-vlan-group sales vlan-name sales_vlan ! vmps-port-group sales_ports device
192.168.2.1 all-ports device 192.168.2.2 port 2/10 device 192.168.2.2 port 2/11 device
192.168.2.2 port 2/12 device 192.168.2.2 port 2/13 device 192.168.2.2 port 2/14 device
192.168.2.2 port 2/15 ! vmps-port-policies vlan-name sales_vlan
port-group sales_ports
!
!!!!!!!!!!!!!! Engineer policy !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- This port policy states that the VMPS checks the MAC address of !--- the PC plugged in
any port in Switch A (192.168.2.1) or Switch C !--- (192.168.2.3) against the MAC addresses
associated to the eng_vlan !--- in the vmps-mac-addr database. ! vmps-vlan-group
engineering vlan-name eng_vlan ! vmps-port-group eng_ports device 192.168.2.1 all-ports
device 192.168.2.3 all-ports ! vmps-port-policies vlan-group engineering
port-group eng_ports

```

!Este error es probablemente el más duro de resolver problemas, porque el Switch VMPS siempre no le dice qué línea contiene los errores. Si la línea configurada no se menciona incorrectamente, intente descargar la base de datos VMPS en las secciones. Por ejemplo, el archivo de muestra de configuración para la Compañía XYZ posee un ejemplo de archivo de base de datos. Si hay un error en el archivo, descargue un archivo que contenga solamente el dominio de los vmps, el modo de los vmps, y las secciones del vmps-mac-addr. Si esta descarga es exitosa, agregue la política de puerto ejecutiva a este archivo y repita la descarga. Continúe hasta que se produzca el error sintáctico, después examinan la sección último-asociada cuidadosamente para saber si hay cualquier Error de configuración. Normalmente, éstos son errores tipográficos.

Nota: Si usted reajusta o acciona el ciclo el Switch del servidor VMPS, la base de datos VMPS descarga del servidor TFTP automáticamente y el VMPS se habilita otra vez. Sin embargo, si usted reajusta o ciclo del poder el servidor TFTP no hay opciones para el respaldo TFTP para el VMPS. Como consecuencia, el Switch continúa utilizando la información docta más reciente del servidor TFTP.

[Clientes de VMPS del Troubleshooting 2900XL/3500XL/2950/3550](#)

El 2900XL, 3500XL, la 2950, y 3550 Catalyst Series Switch pueden todo el actuar como clientes de VMPS. Habilite el comando **debug switch vqpc** de realizar el debugging VMPS en la 2950 y los 3550. Las versiones de Cisco IOS Software Release 12.1(13)EA1 y Posterior apoyan este comando debug. El debugging y el troubleshooting VMPS en los 2900XL y 3500XL Switch se limita al comando **show vmps** y a la interpretación de los mensajes del registro presentados durante los problemas de VMPS. Esta sección describe y explica algunos de los mensajes syslog VMPS más comunes que suelen ocurrir.

```

!--- VMPS domain name must be the same as the VTP domain of the network. !--- This value is case
sensitive. If the VTP domain is TestVmps, the VMPS !--- domain must also be TestVmps. vmps
domain xyz_company ! !--- If the VMPS cannot assign the host a VLAN, shut down the port. If the
!--- VMPS mode is "open," a log message, which states that access is denied !--- is produced and
the port becomes inactive. vmps mode secure ! !--- No fallback VLAN is configured for the XYZ
network, so it is commented out. !--- A fallback VLAN is assigned to a PC whose MAC address is
not present in the !--- database. The fallback VLAN is usually a VLAN where a user cannot access
!--- sensitive network resources. !! vmps fallback nonsecure_vlan ! !--- List of MAC addresses

```

that will be assigned to a VLAN. !--- The VLAN-name matches the names given to VLANs on the VMPS. !--- VLAN names are case sensitive, as is the VMPS domain name. ! !--- MAC address format must be xxxx.xxxx.xxxx . Any other format will not work. !vmps-mac-addr address 0000.0000.0001 vlan-name eng_vlan address 0000.0000.0002 vlan-name eng_vlan address 0000.0000.0003 vlan-name sales_vlan address 0000.0000.0004 vlan-name sales_vlan address 0000.0000.0005 vlan-name executive_vlan address 0000.0000.0006 vlan-name executive_vlan ! !!!!!!!!!!!!!!! Executive policy !!!!!!!!!!!!!!! !--- This port policy states that the VMPS checks the MAC address of the !--- PC plugged in any port in Switch A (192.168.2.1) or port 2/1-5 in !--- Switch B (192.168.2.2) against the MAC addresses associated to the !--- executive_vlan in the vmps-mac-addr database. ! !--- When you create a port group, a range command such as !--- device x.x.x.x port 2/1-5 is not allowed. This will produce !--- a parse error when the VMPS database downloads.

```
vmps-vlan-group executive
vlan-name executive_vlan
!
vmps-port-group executive_ports
device 192.168.2.1 all-ports
device 192.168.2.2 port 2/1
device 192.168.2.2 port 2/2
device 192.168.2.2 port 2/3
device 192.168.2.2 port 2/4
device 192.168.2.2 port 2/5
!
vmps-port-policies vlan-group executive
port-group executive_ports
!
!!!!!!!!!!!!!! Sales policy !!!!!!!!!!!!!!!
!--- This port policy states that the VMPS checks the MAC address !--- of the PC plugged in any
port in Switch A (192.168.2.1) or port !--- 2/10-15 in Switch B (192.168.2.2) against the MAC
addresses associated !--- to the sales_vlan in the vmps-mac-addr database. ! !--- Notice that
you can bind a port group to a VLAN name instead of a !--- VLAN group. A VLAN group allows a
port group to be bound to multiple !--- VLANs. In this case, the ports defined in the port group
sales_port can use !--- the MAC addresses defined in the sales_vlan. vmps-vlan-group sales vlan-
name sales_vlan ! vmps-port-group sales_ports device 192.168.2.1 all-ports device 192.168.2.2
port 2/10 device 192.168.2.2 port 2/11 device 192.168.2.2 port 2/12 device 192.168.2.2 port 2/13
device 192.168.2.2 port 2/14 device 192.168.2.2 port 2/15 ! vmps-port-policies vlan-name
sales_vlan
port-group sales_ports
!
!!!!!!!!!!!!!! Engineer policy !!!!!!!!!!!!!!!
!--- This port policy states that the VMPS checks the MAC address of !--- the PC plugged in any
port in Switch A (192.168.2.1) or Switch C !--- (192.168.2.3) against the MAC addresses
associated to the eng_vlan !--- in the vmps-mac-addr database. ! vmps-vlan-group engineering
vlan-name eng_vlan ! vmps-port-group eng_ports device 192.168.2.1 all-ports device 192.168.2.3
all-ports ! vmps-port-policies vlan-group engineering
port-group eng_ports
!
```

Este mensaje del registro es un mensaje de información, y aparece comúnmente cuando el VMPS rechaza asignar un VLAN al MAC Address especificado. Si esta dirección MAC se debe permitir en el puerto especificado, verifique la configuración de VMPS. Vea el [troubleshooting la sección del archivo de la base de datos VMPS de](#) este documento para más información.

Si un concentrador con varios PC está conectado con un puerto dinámico, usted puede ver varios mensajes VQPCLIENT-2-DENY para los PC conectados con el concentrador. El mensaje VQPCLIENT-2-TOOMANY puede aparecer posteriormente. Cisco recomienda que usted conecta solamente un PC con cada puerto dinámico.

Algún Network Interface Cards (NIC), por ejemplo 3COM 3C574/3C575, puede hacer el Switch presentar en varias ocasiones el mensaje del registro VQPCLIENT-2-DENY. En este caso, actualice a la última versión de controladores NIC para resolver el problema.

Este mensaje aparece cuando el puerto dinámico recibe una explosión de las direcciones MAC que todas se asocian al mismo puerto y el puerto no puede procesar cualquier petición VQP:

```
!--- VMPS domain name must be the same as the VTP domain of the network. !--- This value is case sensitive. If the VTP domain is TestVmps, the VMPS !--- domain must also be TestVmps. vmps domain xyz_company ! !--- If the VMPS cannot assign the host a VLAN, shut down the port. If the !--- VMPS mode is "open," a log message, which states that access is denied !--- is produced and the port becomes inactive. vmps mode secure ! !--- No fallback VLAN is configured for the XYZ network, so it is commented out. !--- A fallback VLAN is assigned to a PC whose MAC address is not present in the !--- database. The fallback VLAN is usually a VLAN where a user cannot access !--- sensitive network resources. !! vmps fallback nonsecure_vlan ! !--- List of MAC addresses that will be assigned to a VLAN. !--- The VLAN-name matches the names given to VLANs on the VMPS. !--- VLAN names are case sensitive, as is the VMPS domain name. ! !--- MAC address format must be xxxx.xxxx.xxxx . Any other format will not work. !vmps-mac-addr address 0000.0000.0001 vlan-name eng_vlan address 0000.0000.0002 vlan-name eng_vlan address 0000.0000.0003 vlan-name sales_vlan address 0000.0000.0004 vlan-name sales_vlan address 0000.0000.0005 vlan-name executive_vlan address 0000.0000.0006 vlan-name executive_vlan !!!!!!!!!!!!!!! Executive policy !!!!!!!!!!!!!!! !--- This port policy states that the VMPS checks the MAC address of the !--- PC plugged in any port in Switch A (192.168.2.1) or port 2/1-5 in !--- Switch B (192.168.2.2) against the MAC addresses associated to the !--- executive_vlan in the vmps-mac-addr database. ! !--- When you create a port group, a range command such as !--- device x.x.x.x port 2/1-5 is not allowed. This will produce !--- a parse error when the VMPS database downloads.
```

```
vmps-vlan-group executive
vlan-name executive_vlan
!
vmps-port-group executive_ports
device 192.168.2.1 all-ports
device 192.168.2.2 port 2/1
device 192.168.2.2 port 2/2
device 192.168.2.2 port 2/3
device 192.168.2.2 port 2/4
device 192.168.2.2 port 2/5
!
vmps-port-policies vlan-group executive
port-group executive_ports
!
!!!!!!!!!!!!!! Sales policy !!!!!!!!!!!!!!!
!--- This port policy states that the VMPS checks the MAC address !--- of the PC plugged in any port in Switch A (192.168.2.1) or port !--- 2/10-15 in Switch B (192.168.2.2) against the MAC addresses associated !--- to the sales_vlan in the vmps-mac-addr database. ! !--- Notice that you can bind a port group to a VLAN name instead of a !--- VLAN group. A VLAN group allows a port group to be bound to multiple !--- VLANs. In this case, the ports defined in the port group sales_port can use !--- the MAC addresses defined in the sales_vlan. vmps-vlan-group sales vlan-name sales_vlan ! vmps-port-group sales_ports device 192.168.2.1 all-ports device 192.168.2.2 port 2/10 device 192.168.2.2 port 2/11 device 192.168.2.2 port 2/12 device 192.168.2.2 port 2/13 device 192.168.2.2 port 2/14 device 192.168.2.2 port 2/15 ! vmps-port-policies vlan-name sales_vlan
port-group sales_ports
!
!!!!!!!!!!!!!! Engineer policy !!!!!!!!!!!!!!!
!--- This port policy states that the VMPS checks the MAC address of !--- the PC plugged in any port in Switch A (192.168.2.1) or Switch C !--- (192.168.2.3) against the MAC addresses associated to the eng_vlan !--- in the vmps-mac-addr database. ! vmps-vlan-group engineering vlan-name eng_vlan ! vmps-port-group eng_ports device 192.168.2.1 all-ports device 192.168.2.3 all-ports ! vmps-port-policies vlan-group engineering
port-group eng_ports
!
```

Este mensaje del registro aparece cuando el mismo puerto se da dos diversas asignaciones VLAN en el plazo de 10 segundos de uno a:

!--- VMPS domain name must be the same as the VTP domain of the network. !--- This value is case sensitive. If the VTP domain is TestVmps, the VMPS !--- domain must also be TestVmps. vmps domain xyz_company ! !--- If the VMPS cannot assign the host a VLAN, shut down the port. If the !--- VMPS mode is "open," a log message, which states that access is denied !--- is produced and the port becomes inactive. vmps mode secure ! !--- No fallback VLAN is configured for the XYZ network, so it is commented out. !--- A fallback VLAN is assigned to a PC whose MAC address is not present in the !--- database. The fallback VLAN is usually a VLAN where a user cannot access !--- sensitive network resources. !! vmps fallback nonsecure_vlan ! !--- List of MAC addresses that will be assigned to a VLAN. !--- The VLAN-name matches the names given to VLANs on the VMPS. !--- VLAN names are case sensitive, as is the VMPS domain name. ! !--- MAC address format must be xxxx.xxxx.xxxx . Any other format will not work. !vmps-mac-addr address 0000.0000.0001 vlan-name eng_vlan address 0000.0000.0002 vlan-name eng_vlan address 0000.0000.0003 vlan-name sales_vlan address 0000.0000.0004 vlan-name sales_vlan address 0000.0000.0005 vlan-name executive_vlan address 0000.0000.0006 vlan-name executive_vlan !!!!!!!!!!!!!!! Executive policy !!!!!!!!!!!!!!! !--- This port policy states that the VMPS checks the MAC address of the !--- PC plugged in any port in Switch A (192.168.2.1) or port 2/1-5 in !--- Switch B (192.168.2.2) against the MAC addresses associated to the !--- executive_vlan in the vmps-mac-addr database. ! !--- When you create a port group, a range command such as !--- device x.x.x.x port 2/1-5 is not allowed. This will produce !--- a parse error when the VMPS database downloads.

```
vmps-vlan-group executive
vlan-name executive_vlan
!
vmps-port-group executive_ports
device 192.168.2.1 all-ports
device 192.168.2.2 port 2/1
device 192.168.2.2 port 2/2
device 192.168.2.2 port 2/3
device 192.168.2.2 port 2/4
device 192.168.2.2 port 2/5
!
vmps-port-policies vlan-group executive
port-group executive_ports
!
!!!!!!!!!!!!!! Sales policy !!!!!!!!!!!!!!!
!--- This port policy states that the VMPS checks the MAC address !--- of the PC plugged in any
port in Switch A (192.168.2.1) or port !--- 2/10-15 in Switch B (192.168.2.2) against the MAC
addresses associated !--- to the sales_vlan in the vmps-mac-addr database. ! !--- Notice that
you can bind a port group to a VLAN name instead of a !--- VLAN group. A VLAN group allows a
port group to be bound to multiple !--- VLANs. In this case, the ports defined in the port group
sales_port can use !--- the MAC addresses defined in the sales_vlan. vmps-vlan-group sales vlan-
name sales_vlan ! vmps-port-group sales_ports device 192.168.2.1 all-ports device 192.168.2.2
port 2/10 device 192.168.2.2 port 2/11 device 192.168.2.2 port 2/12 device 192.168.2.2 port 2/13
device 192.168.2.2 port 2/14 device 192.168.2.2 port 2/15 ! vmps-port-policies vlan-name
sales_vlan
port-group sales_ports
!
!!!!!!!!!!!!!! Engineer policy !!!!!!!!!!!!!!!
!--- This port policy states that the VMPS checks the MAC address of !--- the PC plugged in any
port in Switch A (192.168.2.1) or Switch C !--- (192.168.2.3) against the MAC addresses
associated to the eng_vlan !--- in the vmps-mac-addr database. ! vmps-vlan-group engineering
vlan-name eng_vlan ! vmps-port-group eng_ports device 192.168.2.1 all-ports device 192.168.2.3
all-ports ! vmps-port-policies vlan-group engineering
port-group eng_ports
!
```

Quando ocurre este problema, salga del puerto en el VLA N viejo y borre la dirección MAC que provocó el cambio, para poder volver a aprender el direccionamiento y una nueva petición se pueda enviar al VMPS si transmite otra vez.

Éste es un mensaje informativo y generalmente no indica un problema. Si varios mensajes del

registro del %LINK-3-UPDOWN acompañan este mensaje, marque si el puerto afectado está agitando. Estos mensajes del registro indican un cambio de link en el puerto afectado. En este caso, verifique la conectividad física entre la PC y el puerto switch. Para más información, refiera a la [sección de Troubleshooting de la Capa física de puerto del switch del troubleshooting e interconecte los problemas.](#)

Advertencias VMPS conocidas

Esta tabla enumera las advertencias sabidas VMPS que son útiles cuando usted resuelve problemas el VMPS:

ID de la falla	Síntoma	Resolución
CSCd w2380 7	<p>Cuando la estación terminal se mueve a partir de un puerto de un concentrador a otro puerto en un segundo concentrador (con ambo el Hubs conectado con un switch CatOS, configurado como cliente de VMPS), la estación terminal se niega la asignación de un VLA N. Incluso si la estación terminal está conectada directamente, se niega la dirección MAC.</p>	<p>Solución integrada en 6.3(6), 7.1(2).</p>
CSCdr 09366	<p>El comando set port membership mod/port dynamic en un Supervisor II/III puede fallar y producir el desvío no soportado en el mensaje de error del hardware.</p>	<p>Reparar integrado en 5.5(6),6.2(1),6.1(3).</p>
CSCdp 68303 CSCdr 95115	<p>La descarga VMPS falla y presenta este mensaje de error:</p> <pre>!--- VMPS domain name must be the same as the VTP domain of the network. !--- This value is case sensitive. If the VTP domain is TestVmps, the VMPS !--- domain must also be TestVmps. vmps domain xyz_company ! !--- If the VMPS cannot assign the host a VLAN, shut down the port. If the !--- VMPS mode is "open," a log message, which states that access is denied !--- is produced and the port becomes inactive. vmps mode secure ! !--- No fallback VLAN is configured for the XYZ network, so it is commented out. !--- A fallback VLAN is assigned to a PC whose MAC address is not present in the !--- database. The fallback VLAN is usually a VLAN where a user cannot access !--- sensitive network resources. !! vmps fallback nonsecure_vlan ! !--- List of MAC addresses that will be assigned to a VLAN. !--- The VLAN-</pre>	<p>Solución integrada en 5.4(1), 4.5(6).</p>

```

name matches the names given to
VLANs on the VMPS. !--- VLAN names
are case sensitive, as is the VMPS
domain name. ! !--- MAC address
format must be xxxx.xxxx.xxxx . Any
other format will not work. !vmps-
mac-addr address 0000.0000.0001
vlan-name eng_vlan address
0000.0000.0002 vlan-name eng_vlan
address 0000.0000.0003 vlan-name
sales_vlan address 0000.0000.0004
vlan-name sales_vlan address
0000.0000.0005 vlan-name
executive_vlan address
0000.0000.0006 vlan-name
executive_vlan !!!!!!!!!!!!!!!
Executive policy
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !---
This port policy states that the
VMPS checks the MAC address of the
!--- PC plugged in any port in
Switch A (192.168.2.1) or port 2/1-5
in !--- Switch B (192.168.2.2)
against the MAC addresses associated
to the !--- executive_vlan in the
vmps-mac-addr database. ! !--- When
you create a port group, a range
command such as !--- device x.x.x.x
port 2/1-5 is not allowed. This will
produce !--- a parse error when the
VMPS database downloads.

vmps-vlan-group executive
vlan-name executive_vlan
!
vmps-port-group executive_ports
device 192.168.2.1 all-ports
device 192.168.2.2 port 2/1
device 192.168.2.2 port 2/2
device 192.168.2.2 port 2/3
device 192.168.2.2 port 2/4
device 192.168.2.2 port 2/5
!
vmps-port-policies vlan-group
executive
port-group executive_ports
!
!!!!!!!!!!!!!! Sales policy
!!!!!!!!!!!!!!
!--- This port policy states that
the VMPS checks the MAC address !---
of the PC plugged in any port in
Switch A (192.168.2.1) or port !---
2/10-15 in Switch B (192.168.2.2)
against the MAC addresses associated
!--- to the sales_vlan in the vmps-
mac-addr database. ! !--- Notice
that you can bind a port group to a
VLAN name instead of a !--- VLAN
group. A VLAN group allows a port
group to be bound to multiple !---
VLANs. In this case, the ports
defined in the port group sales_port
can use !--- the MAC addresses

```


	<pre> defined in the sales_vlan. vmps- vlan-group sales vlan-name sales_vlan ! vmps-port-group sales_ports device 192.168.2.1 all- ports device 192.168.2.2 port 2/10 device 192.168.2.2 port 2/11 device 192.168.2.2 port 2/12 device 192.168.2.2 port 2/13 device 192.168.2.2 port 2/14 device 192.168.2.2 port 2/15 ! vmps-port- policies vlan-name sales_vlan port-group sales_ports ! !!!!!!!!!!!!!! Engineer policy !!!!!!!!!!!!!! !--- This port policy states that the VMPS checks the MAC address of !--- the PC plugged in any port in Switch A (192.168.2.1) or Switch C !--- (192.168.2.3) against the MAC addresses associated to the eng_vlan !--- in the vmps-mac-addr database. ! vmps-vlan-group engineering vlan- name eng_vlan ! vmps-port-group eng_ports device 192.168.2.1 all- ports device 192.168.2.3 all-ports ! vmps-port-policies vlan-group engineering port-group eng_ports ! </pre>	
<p>CSCdx 12337</p>	<p>Cuando un teléfono del IP está conectado con un puerto dinámico y un PC está conectado con el teléfono del IP, el cliente de VMPS no puede asignar correctamente un VLA N al PC, si el PC conectado con el teléfono del IP se cambia.</p>	<p>Actualmente, esto es una limitación en el VMPS. El Membresía de DVLAN ocurre solamente cuando un puerto dinámico sale y se une a del Bridge. Si usted cambia el PC conectado con el teléfono del IP y quisiera que el Membresía de</p>

		DVLAN trabajara correctamente, desconecte el teléfono del IP y vuelva a conectar el teléfono del IP al puerto del switch.
CSCds77648	Inundación de zócalo UDP en el zócalo VMPS 1589 tras la reconfirmación o descarga de VMPS. Esto causa un error en la descarga.	Solución integrada en 6.3(1), 5.5(8),4.5(13).
CSCdu19163	Usted no puede fijar el nivel de gravedad del registro a 7 para la ubicación DVLAN en ciertas versiones del software CatOS. Cuando usted fijó el nivel de gravedad del debugging, los estados del Switch que el recurso es inválido, como en este ejemplo: <pre>Console> (enable) set logging level dvlan 7 Invalid Facility Console> (enable)</pre>	Solución integrada en 5.5(9), 6.3(1).
CSCeb36856	A veces, un Catalyst 6000 Switch que ejecuta 7.6(1) no puede asignar dinámicamente sus propios puertos del switch a un VLA N. Cuando ocurre el bug, los puertos permanecen en un estado <code>inactivo</code> .	Arreglo integrado en 7.6(3)

[Información a recolectar antes de que usted entre en contacto el Soporte técnico de Cisco](#)

Para ayudar mejor a los clientes, el Soporte técnico de Cisco pregunta que usted publica estos comandos de obtener la información del cliente de VMPS y del VMPS:

Desde el cliente VMPS

- `show tech-support command log`
- registro del **comando `show logging buffer -1000`** (CatOS)
- registro del **comando `show log`** (Cisco IOS Software)

Desde el cliente VMPS

- show tech-support command log
- una copia del archivo de la base de datos VMPS
- registro del comando **show logging buffer -1000** (CatOS)
- registro del comando **show log** (Cisco IOS Software)

Información Relacionada

- [Solución de problemas del puerto del switch y de la interfaz](#)
- [Configuración del Ruteo de InterVLAN y Trunking de ISL/802.1Q en un Switch Catalyst 2900xl/3500xl/2950 mediante un Router Externo](#)
- [Configurar la membresía VLAN dinámica](#)
- [Páginas de Soporte de Productos de LAN](#)
- [Página de Soporte de LAN Switching](#)
- [Soporte técnico y documentación - Cisco Systems](#)