

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[排除故障DVLAN成员](#)

[在您排除故障DVLAN成员前](#)

[排除故障PC和VMPS客户端交换机之间的连接](#)

[排除故障在VMPS客户端和VMPS之间的连通性问题](#)

[排除故障VMPS数据库文件](#)

[排除故障VMPS数据库文件下载](#)

[排除故障2900XL/3500XL/2950/3550 VMPS客户端](#)


[已知 VMPS 警告](#)

[应收集的信息，在您与思科技术支持联系前](#)

[相关信息](#)

简介

使用VLAN管理策略服务器(VMPS) (VMPS)， Catalyst交换机管理员能动态地分配网络设备到特定VLAN。此技术是有用的在包含很大数量的移动用户的站点。本文包括如何排除故障在的主机注册Catalyst交换机VMPS。主机注册是指VLAN根据PC的以太网MAC地址的能力分配。本文包括必要的最低软件级别运行VMPS和VMPS客户端，并且提供关于怎样的建议排除故障动态VLAN (DVLAN)分配的多种阶段和组件。

注意： Catalyst交换机VMPS只提供主机注册。为了通过NT验证(亦称用户注册)分配VLAN请使用 [Cisco Secure User Registration Tool](#) 。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

此表列出最低软件需求支持在多种Cisco Catalyst交换机产品的VMPS：

产品	VMPS支持	VMPS客户端支持
Catalyst 4000系列(Catalyst OS)	是，7.2(x)及以后	是，所有软件版本

Catalyst 4000/4500 (Cisco IOS软件)	目前不受支持	是， 12.1(13)EW和以后
Catalyst 2900XL/3500XL	不支持	是， 11.2(8)SA4和以后，仅企业软件版本
Catalyst 2950/2955/3550	不支持	是，所有软件版本
Catalyst 2948G-L3/4908G-L3	不支持	不支持
Catalyst 5000/5500家族	是，2.3.x和以后	是， 2.3.x和以后
Catalyst 6000/6500家族 (Catalyst OS)	是，6.1(x)及以后	是，所有软件版本
Catalyst 6000/6500家族 (Cisco IOS软件)	目前不受支持	目前不受支持

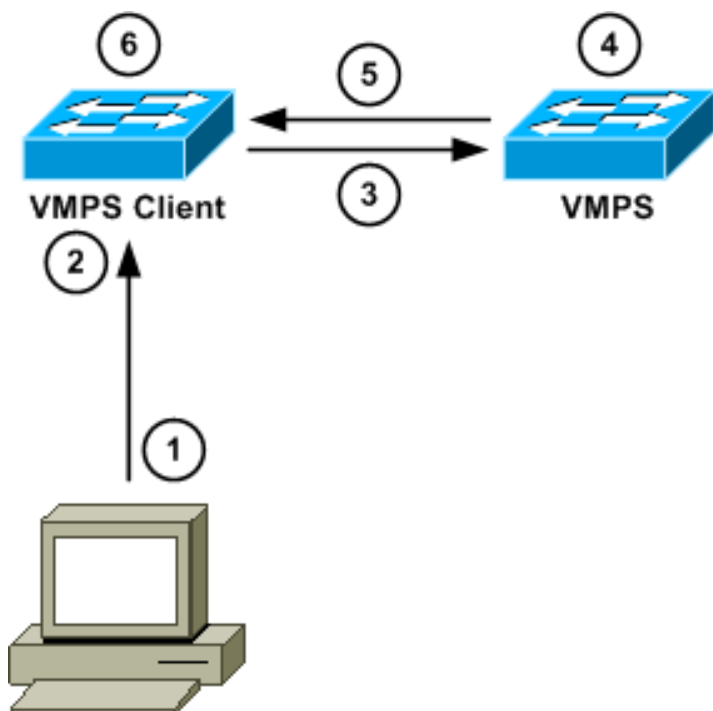
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

排除故障DVLAN成员

VLAN查询协议(VQP)是VMPS数据的主要的传输。VQP用途用户数据报协议(UDP)端口1589。此示例说明在DVLAN成员进程的重要步骤，并且显示客户端如何根据MAC地址动态地分配VLAN：



1. PC发送帧到交换机。
2. VMPS客户端了解在动态端口的PC MAC地址。
3. VMPS客户端发送VQP请求对VMPS。请求包含VMPS客户端IP地址、PC MAC地址、PC端口编号和VTP域。
4. VMPS解析PC VLAN分配的数据库文件。
5. VMPS发送对VMPS客户端的一VQP答复。
6. 如果VQP答复包含VLAN分配，VMPS客户端分配它到VLAN。否则，客户端拒绝PC访问。

您能分类您遇到到这三个类别的多数问题：

- 在PC和VMPS客户端之间的连通性问题。在[排除故障DVLAN成员](#)和[排除故障PC和此的VMPS客户端交换机](#)部分的之间[连接前](#)请参阅文档。
- 在VMPS客户端和VMPS之间的连通性问题。请参阅[VMPS客户端和此VMPS数据库文件](#)文件部分描述的[VMPS](#)和[故障排除之间的故障排除连接](#)。
- VMPS数据库文件配置问题。请参阅[故障排除](#)本文的[VMPS Database File](#)部分。

[在您排除故障DVLAN成员前](#)

在您排除故障在运行Catalyst OS的VMPS客户端前的DVLAN成员问题(CatOS)，请增加在VMPS客户端的DVLAN日志级别从日志级别2对日志级别7 (调试)。然后，请发出**set logging level dvlan 7 default**命令。

注意： 在一些CatOS版本中，当您增加DVLAN日志级别时，错误能出现，阐明，这是一个无效设备。此错误是结果Cisco Bug ID [CSCdu19163](#) ([仅限注册用户](#))，并且此问题在Cisco IOS软件版本被解决5.5(8)，6.3(1)和以后。

您必须启用此on命令VMPS客户端，当您排除故障时，因为此命令提供关于DVLAN成员失败的重要信息。

在您完成故障排除并且解决问题后，您可以降低从日志级别7的DVLAN日志级别到日志级别2.发出**set logging level dvlan 2 default**命令。

在CatOS交换机中，如果发出技术支持工程师，处理的**set trace dynvlan 6**命令您可执行另外的调试。在您接通或电源有VLAN分配问题的前，PC请启用此命令。大约一分钟，在您禁用命令前，请等待。为了禁用命令，请发出**set trace dynvlan 0**命令在特权模式。



警告： 小心地启用此命令。如果几PCs事假和加入动态端口同样的交换，debug输出能引起交换机失败。在您启用此命令前，您必须禁用控制台记录。

[排除故障PC和VMPS客户端交换机之间的连接](#)

如果VMPS客户端交换机不能得到PC的MAC地址，在PC和VMPS客户端之间的连通性问题能造成DVLAN成员发生故障。在这种情况下，端口在保持？非激活？有dyn-VLAN分配的状态，如此示例所显示：

```
vmpls_client> (enable) show port 3/2
Port Name                               Status      Vlan      Level Duplex
Speed Type-----
inactive  dyn-          normal a-half a-10  10/100BaseTX
```

当VMPS再确定在VMPS客户端交换机时发生，并且交换机不能得到任何PC MAC地址在任何动态端口的，然后此消息出现：

```
vmps_client> (enable) show port 3/2Port Name Status Vlan Level Duplex
Speed Type-----
inactive dyn- normal a-half a-10 10/100BaseTX 3/2
```

VMPS再确定发生，当VMPS客户端要求VMPS，如果动态端口分配正确，并且，如果正确MAC地址分配到正确端口。默认情况下，此再确定发生大约每60分钟。发出show vmps命令在VMPS客户端确定VMPS再确认时间。

如果肯定有至少一个PC连接对动态端口，请执行这些步骤：

1. 从交换机断开PC。
2. 发出一ping命令从PC到任何地方。
3. 发出reconfirm vmps命令在连接的VMPS客户端。

VMPS客户端设法确认与VMPS必须分配PC的地址到该端口。如果MAC地址不可能被再确认，此消息出现：

```
vmps_client> (enable) show port 3/2Port Name Status Vlan Level Duplex
Speed Type-----
inactive dyn- normal a-half a-10 10/100BaseTX 3/2
```

问题可以是一问题与VMPS数据库(请参阅[故障排除](#)本文的[VMPS Database File部分](#))或与VMPS客户端和VMPS之间的通信(请参阅本文的[VMPS客户端和VMPS部分](#)的之间[故障排除连接](#))。

如果VMPS客户端交换机继续阐明，没有主机连接对动态端口和再确定中止，请排除故障问题作为在VMPS客户端和PC之间的物理层连通性问题。欲知更多信息，参考[故障排除交换机端口和接口问题物理层故障排除部分](#)。

[排除故障在VMPS客户端和VMPS之间的连通性问题](#)

当失去连接发生在VMPS客户端和VMPS之间时，VMPS再确定能发生故障和生成DVLAN-2-MACNOTRECONFIRMED错误消息。端口丢失DVLAN分配，正如在此示例：

```
vmps_client> (enable) show port 3/2Port Name Status Vlan Level Duplex
Speed Type-----
inactive dyn- normal a-half a-10 10/100BaseTX 3/2
```

VMPS再确定发生，当VMPS客户端要求VMPS，如果动态端口分配正确，并且，如果正确MAC地址分配到正确端口。默认情况下，此检查发生大约每60分钟。发出一show vmps命令在VMPS客户端确定VMPS再确认时间。

完成这些步骤排除故障在VMPS客户端和VMPS之间的连通性问题：

1. ping从VMPS客户端的VMPS。如果ping发生故障，请排除故障问题作为一个一般交换机连接问题或作为一般路由问题。[欲知更多信息，请使用外部路由器在Catalyst 2900XL/3500XL/2950交换机上配置 VLAN间路由和ISL/802.1Q中继。](#)
2. 如果ping命令是成功的在VMPS客户端和VMPS之间，保证没有设备？在VMPS客户端和VMPS网络路径之间？该块UDP端口1589。
3. 如果VMPS客户端和VMPS之间的连接断断续续(丢失的一些数据获得)，您能设法增加在VMPS客户端的VMPS重试间隔，作为应急方案。发出set vmps server retry命令。默认情况下，三倍VMPS客户端尝试。在与间歇接通的一个环境，当您增加VMPS重试间隔时，您给客户端更多机会连接到VMPS，在客户端放弃前，并且VLAN成员发生故障。

[排除故障VMPS数据库文件](#)

VMPS数据库文件定义了控制在Catalyst交换机VMPS的主机注册的所有参数。您必须手工创建有文

本编辑的文件。这些是VMPS数据库的四个主要组件：

- 端口组？在多种交换机找到的端口的一集。
- VLAN组？可以关联对端口组VLAN的一集。
- 端口策略？关联有VLAN组或VLAN名称的端口组。
- 对VLAN关联表的MAC地址？指定对哪个VLAN MAC地址分配。**注意：**您能分配仅MAC地址对一个VLAN。如果您有一个MAC地址与二个不同VLAN相关，只能使用列出的第一个VLAN。**注意：**下案例研究说明VMPS数据库文件如何工作并且帮助您排除故障所有VMPS数据库故障问题。

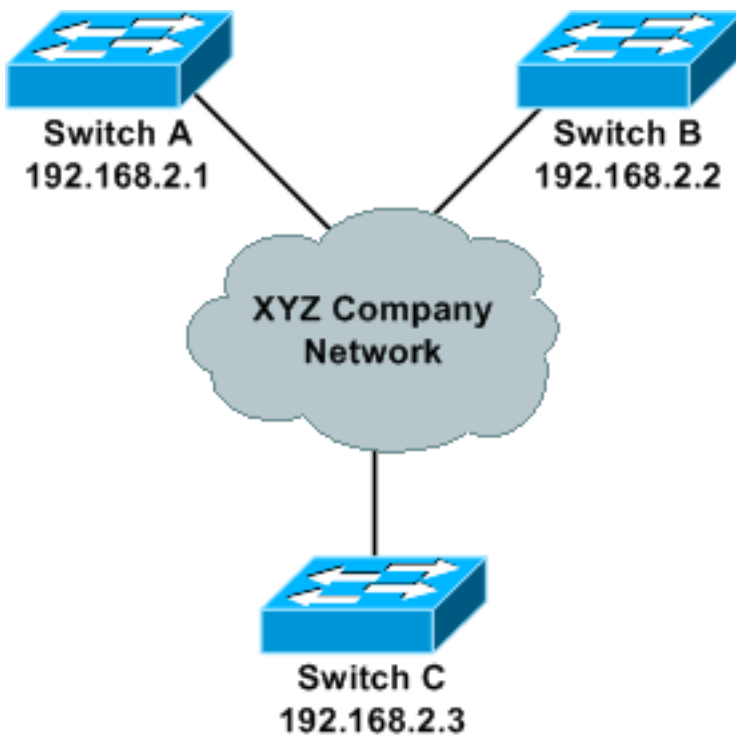
案例研究说明

XYZ公司的有这三个区域：

- 区域1包含培训屋子和设施。
- 区域2是为董事和销售主管。
- 区域3是为工程师。

呼叫的三VLAN？executive_vlan，？??sales_vlan，？并且？eng_vlan？创建。如果他们在他们的办公室或在培训屋子，董事在VLAN executive_vlan必须放置。销售代表所有PCs分配到sales_vlan，并且工程师所有PCs分配到eng_vlan。

这是XYZ公司的设计方案的示例：



交换机	区域	配置
A	培训的区域	董事、销售主管和工程师是授权访问到所有端口和分配到他们的各自的VLAN。

B	塞尔斯/行政区域	仅行政PCs是授权访问到端口2/1-5;行政PCs分配到executive_vlan。仅销售主管PCs访问端口2/10-15;销售主管PCs分配到sales_vlan。对其他端口的访问交换机的拒绝对董事、销售主管和工程师。
C	设计区域	只设计PCs请是授权访问到交换机;设计PCs分配到eng_vlan。

VMPS域名和VTP域名

VMPS域名和VLAN中继协议(VTP)域名必须配比。VMPS域名区分大小写。例如，如果VTP域名是？XYZ_company？VMPS域名必须是？XYZ_company？并且没有？xyz_company？

VMPS端口策略

三个端口策略将创建：第一董事的，第二销售主管的和工程师的第三。

再次，用于的VLAN名称创建VMPS端口策略区分大小写，并且必须匹配在VLAN数据库的VLAN名称。通常，思科建议您使用小写命名所有VLAN和VTP域。

端口策略阐明，高级管理PC连接到交换机B的(192.168.2.2)端口2/1-5或交换机A的(192.168.2.1)所有端口分配到executive_vlan。

端口策略阐明，销售主管PC连接到交换机B的(192.168.2.2)端口2/11-15或交换机A的(192.168.2.1)所有端口分配到sales_vlan。

端口策略阐明，工程师PC连接对交换机A的(192.168.2.1)任何端口或交换机C (192.168.2.3)分配到eng_vlan。

尝试连接到动态端口的其他用户是拒绝访问和端口被关闭。系统消息通知管理员端口关闭，并且适当行为尔后采取。

XYZ公司的此示例VMPS配置文件显示产生的VMPS数据库文件：

```
!--- 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-addraddress 0000.0000.0001 vlan-name
eng_vlanaddress 0000.0000.0002 vlan-name eng_vlanaddress 0000.0000.0003 vlan-name
sales_vlanaddress 0000.0000.0004 vlan-name sales_vlanaddress 0000.0000.0005 vlan-name
executive_vlanaddress 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-
addrs 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 executivevlan-name executive_vlan!vmps-port-group
executive_portsdevice 192.168.2.1 all-portsdevice 192.168.2.2 port 2/1device 192.168.2.2 port
2/2device 192.168.2.2 port 2/3device 192.168.2.2 port 2/4device 192.168.2.2 port 2/5!vmps-port-
policies vlan-group executiveport-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-addrs
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 salesvlan-name sales_vlan!vmps-port-group sales_portsdevice
192.168.2.1 all-portsdevice 192.168.2.2 port 2/10device 192.168.2.2 port 2/11device 192.168.2.2
port 2/12device 192.168.2.2 port 2/13device 192.168.2.2 port 2/14device 192.168.2.2 port
2/15!vmps-port-policies vlan-name sales_vlanport-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-addrs 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!

```

排除故障VMPS数据库文件下载

为了VMPS能正常运行，您必须下载数据库和配置文件从远程拷贝协议(RCP)或简单文件传输协议(TFTP)服务器到VMPS交换机。此进程在这些情况下发生故障：

- 当VMPS数据库文件在RCP或TFTP server不存在也没有不正确地被命名。如果数据库文件在输出中不存在也不匹配数据库文件领域从show vmps命令VMPS交换机，VMPS交换机产生此错误：

```

!--- 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-addrsaddress 0000.0000.0001 vlan-name eng_vlanaddress 0000.0000.0002
vlan-name eng_vlanaddress 0000.0000.0003 vlan-name sales_vlanaddress 0000.0000.0004 vlan-
name sales_vlanaddress 0000.0000.0005 vlan-name executive_vlanaddress 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-addrs 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 executivevlan-name executive_vlan!vmps-port-group executive_portsdevice 192.168.2.1
all-portsdevice 192.168.2.2 port 2/1device 192.168.2.2 port 2/2device 192.168.2.2 port
2/3device 192.168.2.2 port 2/4device 192.168.2.2 port 2/5!vmps-port-policies vlan-group
executiveport-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-addrs 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 salesvlan-name sales_vlan!vmps-port-group
sales_portsdevice 192.168.2.1 all-portsdevice 192.168.2.2 port 2/10device 192.168.2.2 port

```

```

2/11device 192.168.2.2 port 2/12device 192.168.2.2 port 2/13device 192.168.2.2 port
2/14device 192.168.2.2 port 2/15!vmps-port-policies vlan-name sales_vlanport-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!

```

- **当VMPS交换机不能与RCP或TFTP server联系。**如果VMPS交换机不能连接到RCP或TFTP server，VMPS交换机产生此错误：*!--- 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-addraddress 0000.0000.0001 vlan-name eng_vlanaddress 0000.0000.0002 vlan-name eng_vlanaddress 0000.0000.0003 vlan-name sales_vlanaddress 0000.0000.0004 vlan-name sales_vlanaddress 0000.0000.0005 vlan-name executive_vlanaddress 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 executivevlan-name executive_vlan!vmps-port-group executive_portsdevice 192.168.2.1 all-portsdevice 192.168.2.2 port 2/1device 192.168.2.2 port 2/2device 192.168.2.2 port 2/3device 192.168.2.2 port 2/4device 192.168.2.2 port 2/5!vmps-port-policies vlan-group executiveport-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 salesvlan-name sales_vlan!vmps-port-group sales_portsdevice 192.168.2.1 all-portsdevice 192.168.2.2 port 2/10device 192.168.2.2 port 2/11device 192.168.2.2 port 2/12device 192.168.2.2 port 2/13device 192.168.2.2 port 2/14device 192.168.2.2 port 2/15!vmps-port-policies vlan-name sales_vlanport-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!
- 如果VMPS交换机能够联系RCP或TFTP服务器，请注意这是与生产的那个一样的错误，但是数据库文件不存在或者没有正确命名。在这种情况下，您必须验证RCP之间的网络连通性或TFTP server和VMPS交换机。如果网络连通性存在VMPS和VMPS客户端之间，请验证服务器的RCP或TFTP端口是否开放和准备接受连接。

- **当数据库文件包含配置错误。**在下载期间，如果数据库配置错误检测，VMPS交换机产生此错误：*!--- 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-addraddress 0000.0000.0001 vlan-name eng_vlanaddress 0000.0000.0002
vlan-name eng_vlanaddress 0000.0000.0003 vlan-name sales_vlanaddress 0000.0000.0004 vlan-
name sales_vlanaddress 0000.0000.0005 vlan-name executive_vlanaddress 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 executivevlan-name executive_vlan!vmps-port-group executive_portsdevice 192.168.2.1
all-portsdevice 192.168.2.2 port 2/1device 192.168.2.2 port 2/2device 192.168.2.2 port
2/3device 192.168.2.2 port 2/4device 192.168.2.2 port 2/5!vmps-port-policies vlan-group
executiveport-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 salesvlan-name sales_vlan!vmps-port-group
sales_portsdevice 192.168.2.1 all-portsdevice 192.168.2.2 port 2/10device 192.168.2.2 port
2/11device 192.168.2.2 port 2/12device 192.168.2.2 port 2/13device 192.168.2.2 port
2/14device 192.168.2.2 port 2/15!vmps-port-policies vlan-name sales_vlanport-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!

```

此错误很可能是最难排除故障，因为VMPS交换机总是不告诉您哪条线路包含错误。如果配置的线路没有不正确地被提及，请设法下载在部分的VMPS数据库。例如，XYZ公司的示例配置文件有示例数据库文件。如果有在文件的一个错误，请下载只包含VMPS、VMPS和vmps-mac-addr部分的文件。如果此下载成功，则添加管理端口策略到此文件，并重复此下载。请继续，直到解析错误产生，然后仔细检查最后连接部分所有配置错误。通常，这些是印刷错误。

注意： 如果重置或重新通电VMPS服务器交换机，自动从TFTP server下载VMPS数据库，VMPS再次被启用。然而，如果您重置或重新通电TFTP server，则没有为VMPS做TFTP备份的选项。结果，交换机继续使用从TFTP server的最后获知的信息。

[排除故障2900XL/3500XL/2950/3550 VMPS客户端](#)

2900XL、3500XL、2950和3550台Catalyst系列交换机能所有作为VMPS客户端。启用**debug switch vqpc**命令执行调试在2950和3550的VMPS。Cisco IOS软件版本12.1(13)ea1及以上版本版本支持debug命令的此。调试和排除故障在2900XL和3500XL交换机的VMPS对**show vmps**命令和在VMPS问题期间被生成的日志消息的解释被限制。此部分讨论并且说明某些通常被遇到的VMPS系统消息。

```

!--- 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-addraddress 0000.0000.0001 vlan-name eng_vlanaddress 0000.0000.0002 vlan-name eng_vlanaddress 0000.0000.0003 vlan-name sales_vlanaddress 0000.0000.0004 vlan-name sales_vlanaddress 0000.0000.0005 vlan-name executive_vlanaddress 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 executivevlan-name executive_vlan!vmps-port-group executive_portsdevice 192.168.2.1 all-portsdevice 192.168.2.2 port 2/1device 192.168.2.2 port 2/2device 192.168.2.2 port 2/3device 192.168.2.2 port 2/4device 192.168.2.2 port 2/5!vmps-port-policies vlan-group executiveport-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 salesvlan-name sales_vlan!vmps-port-group sales_portsdevice 192.168.2.1 all-portsdevice 192.168.2.2 port 2/10device 192.168.2.2 port 2/11device 192.168.2.2 port 2/12device 192.168.2.2 port 2/13device 192.168.2.2 port 2/14device 192.168.2.2 port 2/15!vmps-port-policies vlan-name sales_vlanport-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!

当VMPS拒绝分配VLAN对指定的MAC地址，此日志消息是供参考消息和通常出现。如果在指定的端口必须允许此MAC地址，请验证VMPS配置。欲知更多信息，请参阅[故障排除](#)本文的[VMPS Database File](#)部分。

如果有几PCs的一台集线器连接到动态端口，您能为PCs看到几个VQPCLIENT-2-DENY消息连接对集线器。VQPCLIENT-2-TOOMANY消息能随后出现。思科建议您只连接一个PC到每个动态端口。

一些网络接口界面卡(NIC)，例如3Com 3C574/3C575，能引起交换机重复生成VQPCLIENT-2-DENY日志消息。在这种情况下，对解决问题的最新的NIC驱动程序的升级。

此消息出现，当动态端口接收全部用相同端口关联，并且端口无法处理所有VQP请求MAC地址的突发流量：

!--- 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-addraddress 0000.0000.0001 vlan-name eng_vlanaddress 0000.0000.0002 vlan-name eng_vlanaddress 0000.0000.0003 vlan-name sales_vlanaddress 0000.0000.0004 vlan-name sales_vlanaddress 0000.0000.0005 vlan-name executive_vlanaddress 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 executivevlan-name executive_vlan!vmps-port-group
executive_portsdevice 192.168.2.1 all-portsdevice 192.168.2.2 port 2/1device 192.168.2.2 port
2/2device 192.168.2.2 port 2/3device 192.168.2.2 port 2/4device 192.168.2.2 port 2/5!vmps-port-
policies vlan-group executiveport-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
s 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 salesvlan-name sales_vlan!vmps-port-group sales_portsdevice
192.168.2.1 all-portsdevice 192.168.2.2 port 2/10device 192.168.2.2 port 2/11device 192.168.2.2
port 2/12device 192.168.2.2 port 2/13device 192.168.2.2 port 2/14device 192.168.2.2 port
2/15!vmps-port-policies vlan-name sales_vlanport-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
s 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!

```

当相同端口在10秒给两个不同的VLAN分配彼此以内时，此日志消息出现：

```

!--- 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
saddress 0000.0000.0001 vlan-name
eng_vlanaddress 0000.0000.0002 vlan-name eng_vlanaddress 0000.0000.0003 vlan-name
sales_vlanaddress 0000.0000.0004 vlan-name sales_vlanaddress 0000.0000.0005 vlan-name
executive_vlanaddress 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
s 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 executivevlan-name executive_vlan!vmps-port-group
executive_portsdevice 192.168.2.1 all-portsdevice 192.168.2.2 port 2/1device 192.168.2.2 port
2/2device 192.168.2.2 port 2/3device 192.168.2.2 port 2/4device 192.168.2.2 port 2/5!vmps-port-
policies vlan-group executiveport-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
s 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 salesvlan-name sales_vlan!vmps-port-group sales_portsdevice
192.168.2.1 all-portsdevice 192.168.2.2 port 2/10device 192.168.2.2 port 2/11device 192.168.2.2
port 2/12device 192.168.2.2 port 2/13device 192.168.2.2 port 2/14device 192.168.2.2 port
2/15!vmps-port-policies vlan-name sales_vlanport-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
s 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!

```

当此问题发生时，请离开旧有VLAN的端口并且删除挑衅更改的MAC地址，因此可以重学地址，并且新要求可以发送到VMPS，如果再传送。

这是供参考消息，并且通常不指示任何问题。如果几%LINK-3-UPDOWN日志消息伴随此消息，请证实受影响的端口是否是飘荡。这些日志消息指示在受影响的端口的链路改变。在这种情况下，PC和交换机端口之间的检查物理连通性。欲知更多信息，参考[故障排除交换机端口和接口问题物理层故障排除部分](#)。

已知 VMPS 警告

此表列出是有用的已知VMPS警告，当您排除故障VMPS时：

Bug ID	症状	解决方法
CSCW23807	当终端站从一台集线器的一个端口对另一个端口的移动第二台集线器的(当两集线器连接对CatOS交换机，配置作为VMPS客户端)，终端站拒绝VLAN的分配。即使终端站直接地连接，MAC地址拒绝。	在6.3(6)集成的修正，7.1(2)。
CSCdr09366	dynamic命令 在Supervisor II/III G能发生故障和导致不 set port membership mod/端口 。	修复集成在5.5(6)，6.2(1)，6.1(3)。
CSCdp683035	VMPS下载发生故障并且生成此错误消息： <i>!--- 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</i>	在5.4(1)集成的修正，4.5(6)。

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_vlanaddress 0000.0000.0002
vlan-name eng_vlanaddress
0000.0000.0003 vlan-name
sales_vlanaddress
0000.0000.0004 vlan-name
sales_vlanaddress
0000.0000.0005 vlan-name
executive_vlanaddress
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 executivevlan-name
executive_vlan!vmps-port-group
executive_portsdevice
192.168.2.1 all-portsdevice
192.168.2.2 port 2/1device
192.168.2.2 port 2/2device
192.168.2.2 port 2/3device
192.168.2.2 port 2/4device
192.168.2.2 port 2/5!vmps-
port-policies vlan-group
executiveport-group
executive_ports!!!!!!!!!!!!!!
Sales policy
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!-
-- This port policy states
that the VMPS checks the MAC

```

1
1
5

	<pre> 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 vmpls- 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 salesvlan-name sales_vlan!vmps-port-group sales_portsdevice 192.168.2.1 all-portsdevice 192.168.2.2 port 2/10device 192.168.2.2 port 2/11device 192.168.2.2 port 2/12device 192.168.2.2 port 2/13device 192.168.2.2 port 2/14device 192.168.2.2 port 2/15!vmps-port-policies vlan-name sales_vlanport-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 vmpls-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>C S C P x 1 2 3 3 7</p>	<p>当IP电话连接到动态端口时，并且PC连接到IP电话，VMPS客户端不能适当地分配VLAN到PC，如果PC连接对IP电话更改。</p>	<p>目前，这是在VMPS的一个限制。只有当动态端口留下并且加入网桥时，DVLAN成员发生。如果更换PC连接对IP电话并且希望DVLAN成员适当地运作，请断开IP电话并且重新连接IP电话到交换机端口。</p>
<p>C</p>	<p>在VMPS socket 1589的UDP</p>	<p>修复集成在6.3(1)，</p>

S C d s 7 7 6 4 8	socket溢出在VMPS再确认或VMPS下载。这造成下载发生故障。	5.5(8) , 4.5(13)。
C S C d u 1 9 1 6 3	您不能设置日志严重级别到7在CatOS软件某些版本的DVLAN设备的。当您设置调试严重级别时，交换机在此示例阐明，设备无效，正如： Console> (enable) set logging level dvlan 7Invalid Facility Console> (enable)	在5.5(9)集成的修正，6.3(1)。
C S C e b 3 6 8 5 6	有时，Catalyst 6000交换机运行的7.6(1)无法动态地分配其自己的交换机端口到VLAN。当bug发生时，端口留在。	修正集成在7.6(3)

[应收集的信息，在您与思科技术支持联系前](#)

为了改善协助客户，思科技术支持要求您发出这些命令从VMPS客户端和VMPS得到信息：

从VMPS客户端

- **show tech-support**命令日志
- **show logging buffer -1000 log**命令(CatOS)
- **show log**命令日志(Cisco IOS软件)

从VMPS

- **show tech-support**命令日志
- VMPS数据库文件的复制
- **show logging buffer -1000 log**命令(CatOS)
- **show log**命令日志(Cisco IOS软件)

[相关信息](#)

- [排除交换机端口及接口问题](#)

- [在 Catalyst 2900XL/3500XL/2950 交换机上使用外部路由器配置 VLAN 间路由和 ISL/802.1Q 中继](#)
- [配置动态VLAN成员](#)
- [LAN 产品支持页](#)
- [LAN 交换技术支持页](#)
- [技术支持和文档- 思科系统](#)