

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Pesquisa defeitos a sociedade DVLAN](#)

[Antes que você pesquisar defeitos a sociedade DVLAN](#)

[Pesquisa defeitos a Conectividade entre o PC e o interruptor do cliente de VMPS](#)

[Pesquisa defeitos problemas de conectividade entre o cliente de VMPS e o VMPS](#)

[Pesquisa defeitos o arquivo de banco de dados de VMPS](#)

[Pesquisa defeitos o download de arquivo de banco de dados vmpls](#)

[Pesquisa defeitos os clientes de VMPS 2900XL/3500XL/2950/3550](#)


[Caveats conhecidos de VMPS](#)

[Informação a recolher antes que você contactar o Suporte técnico de Cisco](#)

[Informações Relacionadas](#)

[Introdução](#)

Com o VLAN Management Policy Server (VMPS), um switch Catalyst pode atribuir dinamicamente um dispositivo de rede a uma VLAN específica. Esta tecnologia é útil em locais com um grande número de usuários móveis. Este documento descreve como resolver problemas de registo do host em um VMPS de um switch Catalyst. O registo do host refere-se à capacidade de atribuir uma VLAN com base no endereço MAC Ethernet de um PC. Este documento discute o nível de software mínimo necessário para executar o VMPS e o cliente VMPS e oferece sugestões de como resolver problemas nas várias fases e nos componentes de uma atribuição de Dynamic VLAN (DVLAN).

Nota: O VMPS de Catalyst switch fornece somente o registo do host. A fim atribuir um VLAN com a autenticação de NT (igualmente conhecida como o registo de usuário) use a [Ferramenta Cisco Secure User Registration](#) .

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

Esta tabela alista os requisitos de software mínimo para apoiar o VMPS em vários produtos de switch do Cisco catalyst:

Produto	Suporte de VMPS	Suporte de Cliente VMPS
Catalyst 4000 Family (OS do catalizador)	Sim, 7.2(x) e mais atrasado	Sim, todos os software release
Catalizador 4000/4500 (Cisco IOS Software)	Apoiado não atualmente	Sim, 12.1(13)EW e mais tarde
Catalyst 2900XL/3500XL	Não suportado	Sim, 11.2(8)SA4 e mais tarde, edição do software de empreendimento somente
Catalyst 2950/2955/3550	Não suportado	Sim, todos os software release
Catalyst 2948G-L3/4908G-L3	Não suportado	Não suportado
Família Catalyst 5000/5500	Sim, 2.3.x e mais tarde	Sim, 2.3.x e mais tarde
Família do Catalyst 6000/6500 (OS do catalizador)	Sim, 6.1(x) e mais atrasado	Sim, todos os software release
Família do Catalyst 6000/6500 (Cisco IOS Software)	Apoiado não atualmente	Apoiado não atualmente

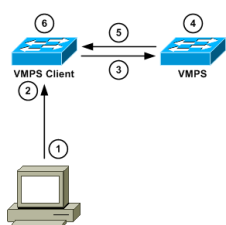
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Pesquise defeitos a sociedade DVLAN

O VQP (VLAN Query Protocol) é o principal transporte para dados VMPS. O VQP usa o User Datagram Protocol (UDP), porta 1589. Este exemplo ilustra as etapas importantes no processo da sociedade DVLAN, e mostra como um cliente é atribuído dinamicamente um VLAN com base no MAC address:



1. O PC envia um quadro ao interruptor.
2. O cliente de VMPS aprende o MAC address PC na porta dinâmica.
3. O cliente de VMPS envia um pedido VQP ao VMPS. O pedido contém o endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente de VMPS, o MAC address PC, o número de porta de PC, e o VTP domain.
4. Os parâmetros de VMPS o arquivo da base de dados para a atribuição de VLAN PC.
5. O VMPS envia uma resposta VQP ao cliente de VMPS.
6. Se a resposta VQP contém uma atribuição de VLAN, o cliente de VMPS atribui-a ao VLAN. Se não, o cliente nega o acesso de PC.

Você pode classificar a maioria de problemas que você encontra nestas três categorias:

- Problemas de conectividade entre o PC e o cliente de VMPS. Veja [antes pesquisando defeitos da sociedade DVLAN](#) e [pesquisando defeitos a Conectividade entre o PC e as seções do interruptor do cliente de VMPS](#) deste documento.
- Problemas de conectividade entre o cliente de VMPS e o VMPS. Veja que a [Conectividade do Troubleshooting entre o cliente de VMPS e o VMPS](#) e o [Troubleshooting que as seções de arquivo do banco de dados de VMPS](#) desta documentam.
- Problemas da configuração de arquivos do banco de dados de VMPS. Veja o [Troubleshooting a seção de arquivo do banco de dados de VMPS](#) deste documento.

Antes que você pesquisar defeitos a sociedade DVLAN

Antes que você pesquisar defeitos problemas da sociedade DVLAN em um cliente de VMPS que execute o OS do catalizador (CatOS), aumente o nível de registro DVLAN no cliente de VMPS do nível de registro 2 ao nível de registro 7 (eliminação de erros). Então, emita o **comando set logging level dvlan 7 default**.

Nota: Em algumas liberações de CatOS, quando você aumenta o nível de registro DVLAN, um erro pode ocorrer, que indique que esta é uma facilidade inválida. Este erro é um resultado da identificação de bug Cisco [CSCdu19163 \(clientes registrados somente\)](#), e esta edição é resolvida nos Cisco IOS Software Release 5.5(8), 6.3(1), e mais tarde.

Você deve permitir este comando em clientes de VMPS quando você pesquisa defeitos porque este comando fornece a informação vital sobre a falha da sociedade DVLAN.

Depois que você termina o Troubleshooting e resolve a edição, você pode reduzir o nível de registro DVLAN do nível de registro 7 à edição do nível de registro 2. o **comando set logging level dvlan 2 default**.

Nos switch CatOS, você pode executar a eliminação de erros adicional se você emite o **comando set trace dynvlan 6** dirigido por um engenheiro de suporte técnico. Permita este comando antes que você obstrua dentro ou ponha acima o PC com edições da atribuição de VLAN. Espere aproximadamente um minuto antes que você desabilite o comando. A fim desabilitar o comando, emita o **comando set trace dynvlan 0** no modo enable.



Cuidado: Permita este comando com cuidado. O resultado do debug pode fazer com que o interruptor cause um crash, se diversos PC saem e se juntam a portas dinâmica no mesmo interruptor. Você deve desabilitar o logging de console antes que você permita este comando.

[Pesquise defeitos a Conectividade entre o PC e o interruptor do cliente de VMPS](#)

Os problemas de conectividade entre o PC e o cliente de VMPS podem fazer com que a sociedade DVLAN falhe se o interruptor do cliente de VMPS não pode obter o MAC address do PC. Neste caso, a porta permanece no? inativo? estado com uma atribuição de VLAN de *dyn*, segundo as indicações deste exemplo:

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

Quando uma reconfirmação de VMPS ocorre no interruptor do cliente de VMPS e o interruptor não pode obter o MAC address de nenhum PC em nenhuma porta dinâmica, a seguir esta mensagem aparece:

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

A reconfirmação de VMPS ocorre quando o cliente de VMPS pede o VMPS se as atribuições de porta dinâmica estão corretas e se os endereços corretos MAC estiveram atribuídos às portas corretas. À revelia, este reconfirmation ocorre sobre cada 60 minutos. Emita o comando `show vmpls` no cliente VMPS para determinar o tempo de reconfirmação do VMPS.

Se você é certo que há pelo menos um PC conectado a uma porta dinâmica, execute estas etapas:

1. Desligue o PC do interruptor.
2. Emita um **comando ping do PC** a em qualquer lugar.
3. Emita o **comando reconfirm vmpls** no cliente de VMPS de conexão.

O cliente de VMPS tenta confirmar com o VMPS que o endereço do PC deve ser atribuído a essa porta. Se o MAC address não pode ser reconfirmado, esta mensagem aparece:

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

A edição pode ser um problema com o banco de dados de VMPS (veja o [Troubleshooting a seção de arquivo do banco de dados de VMPS](#) deste documento) ou com uma comunicação entre o cliente de VMPS e o VMPS (veja a [Conectividade do Troubleshooting entre o cliente de VMPS e a seção VMPS](#) deste documento).

Se o interruptor do cliente de VMPS continua a indicar que não há nenhum host conectado à porta dinâmica, e os abortos do reconfirmation, pesquise defeitos a edição como um problema de conectividade da camada física entre um cliente de VMPS e um PC. Para mais informação, refira a [seção de Troubleshooting da camada física da porta de switch do Troubleshooting e conecte problemas](#).

[Pesquise defeitos problemas de conectividade entre o cliente de VMPS e o VMPS](#)

Quando uma perda de conectividade ocorre entre um cliente de VMPS e um VMPS, a reconfirmação de VMPS pode falhar e produzir o Mensagem de Erro `DVLAN-2-MACNOTRECONFIRMED`. A porta perde a atribuição de DVLAN, como neste exemplo:

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

inactive dyn- normal a-half a-10 10/100BaseTX

A reconfirmação de VMPS ocorre quando o cliente de VMPS pede o VMPS se as atribuições de porta dinâmica estão corretas e se os endereços corretos MAC estiveram atribuídos às portas direitas. À revelia, esta verificação ocorre sobre cada 60 minutos. Emita um **comando show vmps** no cliente de VMPS determinar o tempo da reconfirmação de VMPS.

Termine estas etapas para pesquisar defeitos problemas de conectividade entre um cliente de VMPS e um VMPS:

1. Execute o ping do VMPS a partir do cliente VMPS. Se o sibilo falha, pesquise defeitos o problema como uma edição geral da conectividade de switch ou como um problema de roteamento geral. Para obter mais informações, consulte [.Configurando o roteamento InterVLAN e o entroncamento ISL/802.1Q em um Switch Catalyst 2900XL/3500XL/2950 com um roteador externo.](#)
2. Se o **comando ping** é bem sucedido entre o cliente de VMPS e o VMPS, assegure-se de que não haja nenhum dispositivo? entre o cliente de VMPS e o caminho de rede VMPS? essa porta 1589 dos blocos UDP.
3. Se a Conectividade entre o cliente de VMPS e o VMPS é intermitente (alguns dados obtêm perdidos ao longo do caminho), você pode tentar aumentar o intervalo de nova tentativa VMPS no cliente de VMPS, como uma ação alternativa. Emita o **comando set vmps server retry**. À revelia, o cliente de VMPS tenta extremamente. Em um ambiente com conectividade intermitente, quando você aumenta o intervalo de nova tentativa VMPS, você dá ao cliente mais possibilidades conectar ao VMPS antes que o cliente dê acima e a sociedade de VLAN falhar.

[Pesquise defeitos o arquivo de banco de dados de VMPS](#)

O arquivo de banco de dados de VMPS define todos os parâmetros que registro do host do controle no VMPS de Catalyst switch. Você deve manualmente criar o arquivo com um editor de texto. Estes são os quatro componentes principais do banco de dados de VMPS:

- Grupo de porta? Uma coleção das portas encontradas no vário Switches.
- Grupo vlan? uma coleção de VLANs que pode ser associado a um grupo de portas.
- Política da porta? associa um grupo de porta a um grupo ou nome de VLAN.
- MAC address à tabela de associação VLAN? Especifica a que VLAN um MAC address é atribuído. **Nota:** Você pode atribuir um MAC address somente a um VLAN. Se tiver um endereço MAC associado a duas VLANs diferentes, somente o primeiro listado é usado. **Nota:** Os Casos Práticos seguintes ilustram como o arquivo de banco de dados de VMPS funciona e ajudam-no a pesquisar defeitos toda a edição da falha do banco de dados de VMPS.

Descrição dos Casos Práticos

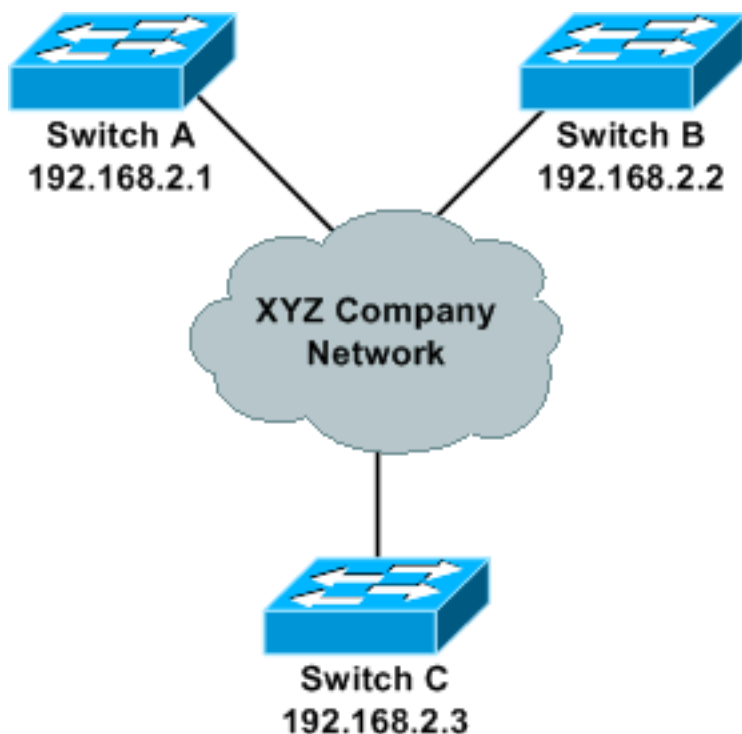
A empresa XYZ tem estas três áreas:

- A área 1 contém as salas e as facilidades do treinamento.
- A área 2 é para executivos e representantes de vendas.
- A área 3 é para coordenadores.

Três VLAN chamados? executive_vlan? ? sales_vlan? e? eng_vlan? são criados. Os executivos

devem ser postos sobre o VLAN `executive_vlan`, se estão em seu escritório ou na sala do treinamento. Todos os PC do representante de vendas são atribuídos ao `sales_vlan`, e todos os PC dos coordenadores são atribuídos ao `eng_vlan`.

Este é um exemplo do esquema do projeto da empresa XYZ:



Switch	Área	Configuração
A	Área de formação	Os executivos, os representantes de vendas, e os coordenadores são concedidos o acesso a todas as portas e atribuídos a seus VLAN respectivos.
B	Vendas/área executiva	Somente os PC executivos são concedidos o acesso à porta 2/1-5; o executivo PC é atribuído a <code>executive_vlan</code> . Somente o representante de vendas PC tem o acesso à porta 2/10-15; o representante de vendas PC é atribuído a <code>sales_vlan</code> . O acesso a outras portas no interruptor é negado aos executivos, aos representantes de vendas, e aos coordenadores.
C	Projetando a área	Somente projetando PC são concedidos o acesso ao interruptor; projetando PC são atribuídos a <code>eng_vlan</code> .

Nome de Domínio VMPS e Nome de Domínio VTP

O Domain Name VMPS e o Domain Name do protocolo VLAN Trunk (VTP) devem combinar. O nome de domínio VMPS faz diferenciação entre maiúsculas e minúsculas. Por exemplo, se o Domain Name VTP é? XYZ_company? , o Domain Name VMPS deve ser? XYZ_company? e não? xyz_company.?

Política de portas do VMPS

Três políticas da porta serão criadas: o primeiro para executivos, o segundo para representantes de vendas, e o terceiro para coordenadores.

Além disso, os nomes VLAN usados para criar as políticas da porta VMPS são diferenciando maiúsculas e minúsculas e devem combinar o nome VLAN na base de dados de VLAN. Em regra geral, Cisco recomenda que você usa a caixa baixa para nomear todos os VLAN e VTP domain.

A política da porta do `executivo` indica que um executivo PC conectou à porta 2/1-5 no switch B (192.168.2.2) ou toda a porta no Switch A (192.168.2.1) é atribuída a `executive_vlan`.

A política da porta das `vendas` indica que um representante de vendas PC conectou à porta 2/11-15 no switch B (192.168.2.2) ou toda a porta no Switch A (192.168.2.1) é atribuída a `sales_vlan`.

A política da porta da `engenharia` indica que um coordenador PC conectado a alguma porta no Switch A (192.168.2.1) ou o C do interruptor (192.168.2.3) é atribuído a `eng_vlan`.

Todos usuários restantes que tentam conectar às portas dinâmica são negados o acesso e a porta são fechados. Um mensagem do syslog informa o administrador da parada de porta, e a ação apropriada é tomada depois disso.

Este arquivo de configuração VMPS da amostra para a empresa XYZ mostra o arquivo de banco de dados de 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-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
```


- Quando o interruptor VMPS não puder contactar o RCP ou o servidor TFTP. Se o interruptor VMPS não pode conectar ao RCP ou ao servidor TFTP, o interruptor VMPS produz este

```
erro:!--- 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!
```

Observe que este é o mesmo erro que esse produzido se o interruptor VMPS pode contactar o RCP ou o servidor TFTP, mas o arquivo da base de dados não existe nem está nomeado incorretamente. Neste caso, você deve verificar a conectividade de rede entre o RCP ou o servidor TFTP e o interruptor VMPS. Se a conectividade de rede existe entre o VMPS e o cliente de VMPS, verifique se a porta RCP ou TFTP do server está aberta e pronta para receber conexões.

- Quando o arquivo da base de dados contiver erros de configuração. Se um erro da configuração do banco de dados é detectado durante a transferência, o interruptor VMPS produz este erro:!--- 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!

```

Este erro é provavelmente o mais duro de pesquisar defeitos, porque o interruptor VMPS não lhe diz sempre que linha contém os erros. Se a linha configurada não é mencionada incorretamente, tente transferir o banco de dados de VMPS nas seções. Por exemplo, o arquivo de configuração de exemplo da Empresa XYZ tem um arquivo de banco de dados de exemplo. Se há um erro no arquivo, transfira um arquivo que contenha somente o domínio dos vmps, o modo dos vmps, e as seções do Vmps-mac-addr. Se este download for bem sucedido, adicionar a política de porta executiva a este arquivo e repetir o download. Continue até que o erro de análise esteja produzido, a seguir inspecionam a seção último-anexada com cuidado para todos os erros de configuração. Normalmente, são erros tipográficos.

Nota: Se você restaura ou põe o ciclo o interruptor do servidor de VMPS, o banco de dados de VMPS transfere do servidor TFTP automaticamente e o VMPS é permitido outra vez. Contudo, se você restaura ou ciclo da potência o servidor TFTP não há nenhuma opção de backup de TFTP para o VMPS. Em consequência, o interruptor continua a usar a última informação instruída do servidor TFTP.

[Pesquise defeitos os clientes de VMPS 2900XL/3500XL/2950/3550](#)

O 2900XL, 3500XL, a 2950, e 3550 Catalyst series switch podem todo o atuar como clientes de VMPS. Permita o **comando debug switch vqpc** executar a eliminação de erros VMPS na 2950 e nos 3550. As versões de Cisco IOS Software Release 12.1(13)EA1 e Mais Recente apoiam este comando debug. A eliminação de erros e o Troubleshooting VMPS nos 2900XL e 3500XL Switch são limitados ao **comando show vmps** e à interpretação dos mensagens de registro produzidos durante problemas com VMPS. Esta seção discute e explica algumas das mensagens de syslog do VMPS mais comuns.

!--- 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!

```

Este mensagem de registro é um mensagem informativa, e aparece geralmente quando o VMPS recusa atribuir um VLAN ao endereço de MAC especificado. Se este MAC address deve ser permitido na porta especificada, verifique a configuração VMPS. Veja o [Troubleshooting a seção de arquivo do banco de dados de VMPS](#) deste documento para mais informação.

Se um hub com diversos PC é conectada a uma porta dinâmica, você pode ver diversas mensagens VQPCLIENT-2-DENY para os PC conectados ao hub. A mensagem VQPCLIENT-2-TOOMANY pode aparecer subsequentemente. Cisco recomenda que você conecta somente um PC a cada porta dinâmica.

Algum Network Interface Cards (NIC), como o 3Com 3C574/3C575, pode fazer com que o interruptor produza repetidamente o mensagem de registro VQPCLIENT-2-DENY. Neste caso, atualize para os drivers de NIC mais recentes para resolver o problema.

Esta mensagem aparece quando a porta dinâmica recebe uma explosão dos endereços MAC que todos estão associados com a mesma porta e a porta é incapaz de processar todo o pedido 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-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!

```

Este mensagem de registro aparece quando a mesma porta é dada duas atribuições de VLAN diferentes dentro dos segundos 10 de se:

```

!--- 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!

```

Quando este problema ocorre, deixe a porta no VLAN velho e suprima do MAC address que provocou a mudança, de modo que o endereço pudesse ser relearned e um pedido novo pudesse ser enviado ao VMPS se transmite outra vez.

Esta é uma mensagem informativa e geralmente não indica nenhum problema. Se diversos mensagens de registro do %LINK-3-UPDOWN acompanham esta mensagem, verifique se a porta afetada esteja batendo. Estes mensagens de registro indicam uma alteração de link na porta afetada. Neste caso, conectividade física da verificação entre o PC e a porta de switch. Para mais informação, refira a [seção de Troubleshooting da camada física da porta de switch do Troubleshooting e conecte problemas](#).

Caveats conhecidos de VMPS

Esta tabela alista as advertências conhecidas VMPS que são úteis quando você pesquisa defeitos o VMPS:

ID do bug	Sintoma	Resolução
CSCdw23807	Quando a estação final estiver movida de uma porta de um hub para uma outra porta em um segundo hub (com ambos os Hubs conectado a um switch CatOS, configurado como um cliente de VMPS), a estação final está negada a atribuição de um VLAN. Mesmo se a estação final é conectada diretamente, o MAC address é negado.	Correção integrada nas versões 6.3(6) e 7.1(2).
CSCdr09366	O comando set port membership mod/port dynamic em um Supervisor II/III G pode falhar e produzir a armadilha não apoiada no mensagem de erro de hardware.	Correção integrada no 5.5(6), 6.2(1), 6.1(3).
CSCdp68303 CSCdr951	A transferência VMPS falha e produz este Mensagem de Erro: !---	Correção integrada em 5.4(1), 4.5(6).

```

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.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-
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 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

```

	<pre> 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! </pre>	
<p>CSCdx12337</p>	<p>Quando um telefone IP está conectado a uma porta dinâmica e um PC está conectado ao telefone IP, o cliente de VMPS não pode corretamente atribuir um VLAN ao PC, se o PC conectado ao telefone IP é mudado.</p>	<p>Atualmente, esta é uma limitação no VMPS. A sociedade DVLAN ocorre somente quando uma porta dinâmica sae e se junta à ponte. Se você muda o PC conectado ao telefone IP e quer a sociedade DVLAN trabalhar corretamente, desligue o telefone IP e reconecte o telefone IP à porta de switch.</p>

CSCds77648	<p>Excesso de soquete UDP no soquete 1589 de VMPS após vmps reconfirm ou vmps download. Isso causa falhas no download.</p>	<p>Correção integrada nas versões 6.3(1), 5.5(8),4.5(13).</p>
CSCdu19163	<p>Você não pode ajustar o nível de seriedade do log a 7 para a facilidade de DVLAN em determinadas versões de CatOS Software. Quando você ajusta o nível de seriedade da eliminação de erros, o interruptor indica que a facilidade é inválida, como neste exemplo: Console> (enable) set logging level dvlan 7Invalid FacilityConsole> (enable)</p>	<p>Correção integrada à versão 5.5(9), 6.3(1).</p>
CSCeb36856	<p>Às vezes, um Catalyst 6000 Switch que execute 7.6(1) é incapaz de atribuir dinamicamente suas próprias portas de switch a um VLAN. Quando o erro ocorre, as portas permanecem em um estado <code>inativo</code>.</p>	<p>Reparo integrado em 7.6(3)</p>

[Informação a recolher antes que você contactar o Suporte técnico de Cisco](#)

A fim ajudar melhor a clientes, o Suporte técnico de Cisco pergunta que você emite estes comandos obter a informação do cliente de VMPS e do VMPS:

A partir do cliente VMPS

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

Do VMPS

- registro do comando `show tech-support`
- uma cópia do arquivo do banco de dados VMPS
- log do comando `show logging buffer -1000` (CatOS)
- log do comando `show log` (Cisco IOS Software)

Informações Relacionadas

- [Troubleshooting de Portas de Switches e Interfaces](#)
- [Configuração do Roteamento entre VLANs e o Entroncamento de ISL/802.1Q em um Switch Catalyst 2900XL/3500XL/2950 Utilizando um Roteador Externo](#)
- [Configurando a associação de vlan dinâmica](#)
- [Páginas de Suporte de Produtos de LAN](#)
- [Página de suporte da switching de LAN](#)
- [Suporte técnico e documentação - Cisco Systems](#)