使用 Catalyst 交换机配置 VLAN 间路由

目录

简介

先决条件

- 要求
- 使用的组件
- 规则
- 相关产品

背景信息

配置

- 网络图
  - 实用提示
- 配置

验证

- Catalyst 3850
- Catalyst 4500-A
- Catalyst 4500-B

故障排除

- 故障排除步骤

相关信息

简介

本文档介绍如何使用 Cisco Catalyst 系列交换机配置 VLAN 间路由。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 了解如何创建 VLAN

  有关详细信息，请参阅在Catalyst交换机上创建以太网VLAN。

- 了解如何创建中继链路

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行Cisco IOS® XE软件版本16.12.7的Catalyst 3850

- 运行Cisco IOS®软件版本03.09.00E的Catalyst 4500

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。如果您的网络处于活动状态，请确保您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。

相关产品

此配置也可用于以下硬件和软件版本：

- 任何Catalyst 3k/9k交换机及更高版本
- 任何Catalyst交换机型号，用作接入层交换机

背景信息

本文档提供典型网络场景下Catalyst 3850系列交换机的VLAN间路由配置示例。本文档使用两个Catalyst 4500系列交换机作为直接连接到Catalyst 3850的第2层(L2)交换机。Catalyst 3850配置还有一条默认路由，用于在下一跳指向Cisco路由器时所有流量到达Internet。可以用防火墙或其它路由器型号替换Internet网关。

注意：来自Internet网关路由器的配置不相关，因此本文档不介绍配置。

在交换网络中，VLAN 将设备分入不同的冲突域和第三层 (L3) 子网内。同一 VLAN 内的设备能相互通信，无需路由。不同VLAN中的设备需要路由设备相互通信。

仅L2交换机需要L3路由设备来提供VLAN之间的通信。该设备可以在交换机外部，也可以是在同一个机箱的另一个模块中。一种新型的交换机将路由功能整合到了交换机内。其中的一个例子就是3850。交换机接收数据包，确定数据包属于另一个VLAN，然后将数据包发送到目的VLAN上的相应端口。

典型的网络设计根据设备所属的组或功能分割网络。例如，工程 VLAN 只有与工程部相关的设备，财务 VLAN 只有与财务相关的设备。如果启用路由，每个 VLAN 中的设备就能够相互通信，无需所有的设备处于同一个广播域中。这样的 VLAN 设计也有其他好处。该设计允许管理员使用访问列表限制 VLAN 间的通信。例如，您可以使用访问列表限制工程VLAN访问财务VLAN上的设备。

有关详细信息，请参阅本文档说明如何在Catalyst 3550系列交换机上配置VLAN间路由，请参阅如何在第3层交换机上配置VLAN间路由。

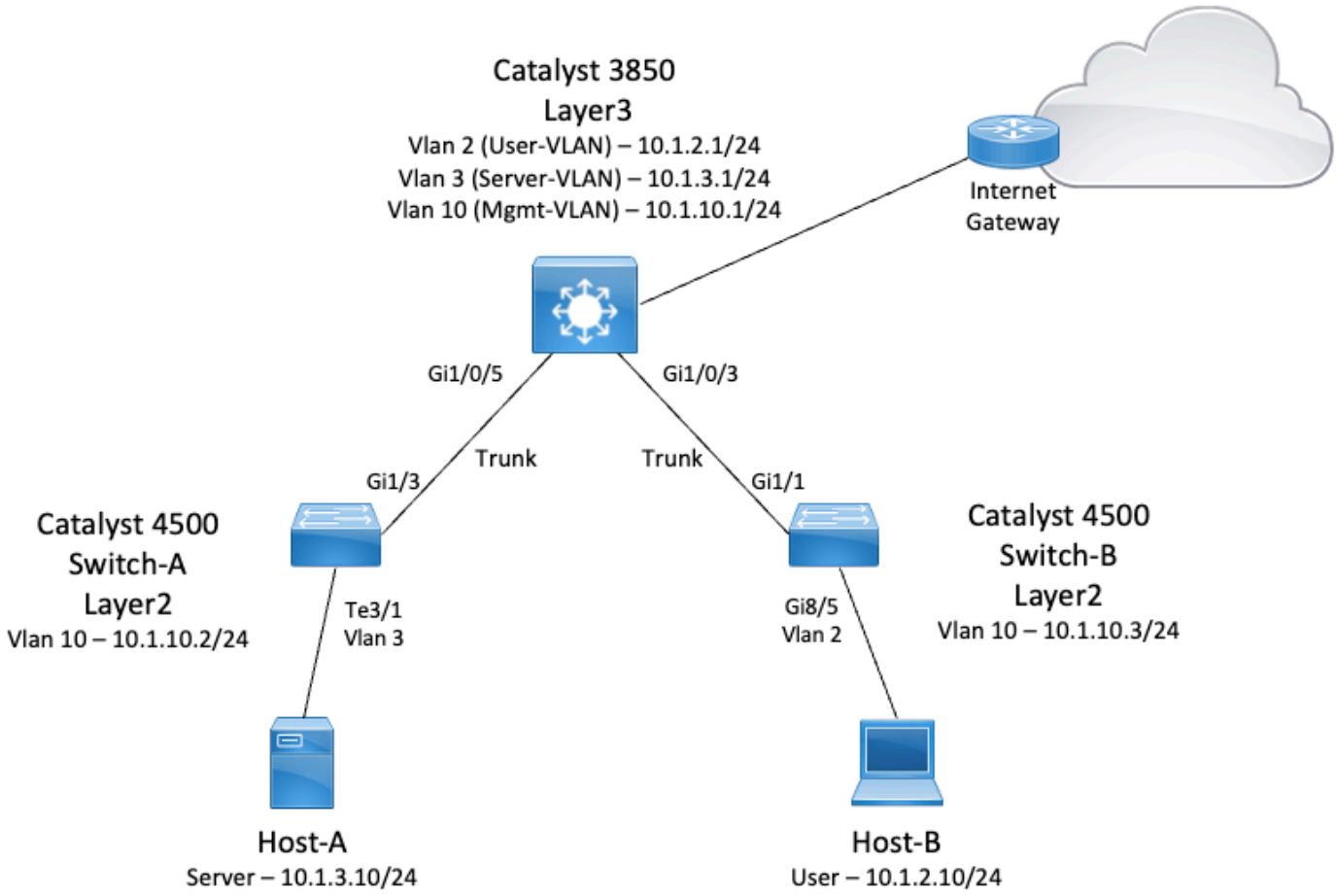
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用Cisco支持工具查找有关此处所用命令的详细信息。只有注册思科用户才能访问此类工具和其他内部信息。

网络图

本文档使用以下网络设置：



在此图中，Catalyst 3850的小型示例网络提供各个网段之间的VLAN间路由。Catalyst 3850交换机可以用作禁用IP路由的第2层设备。为了使交换机用作L3设备并提供VLAN间路由，请确保全局启用IP路由。

以下是用户定义的3个VLAN:

- VLAN 2 — 用户VLAN
- VLAN 3 — 服务器VLAN
- VLAN 10 — 管理VLAN

每个服务器和主机设备上的默认网关配置必须是 3850 上对应的 VLAN 接口 IP 地址。例如，对于服务器，默认网关为10.1.3.1。接入层交换机（即Catalyst 4500）中继到Catalyst 3850交换机。

Catalyst 3850的默认路由指向Cisco路由器，用于路由发往Internet的流量。因此，3850在路由表中没有路由的流量会转发到Cisco路由器进行其他处理。

实用提示

- 确保 802.1Q 中继的中继链路两端的本地 VLAN 相同。如果位于中继一端的本地 VLAN 与另一端的本地 VLAN 不相同，则这两端的本地 VLAN 数据流将无法在中继上正确传输。这种传输故障可能会导致网络出现某些连接问题。
- 如上图所示，将管理 VLAN 与用户 VLAN 或服务器 VLAN 分离。管理 VLAN 与用户 VLAN 或服务器 VLAN 不同。如此分离后，在用户 VLAN 或服务器 VLAN 上发生的任何广播/数据包风暴都不会影响交换机的管理。
- 请勿使用 VLAN 1 进行管理。Catalyst交换机中的所有端口都默认为VLAN 1，而连接到未配置端口的所有设备都位于VLAN 1中。使用VLAN 1进行管理可能会导致交换机管理出现潜在问题。
- 请使用第 3 层（路由）端口连接到默认网关端口。在本例中，您可以轻松地将思科路由器替换为连接到互联网网关路由器的防火墙。
- 本示例在3850上配置一条指向Cisco路由器的静态默认路由以访问Internet。如果只有一个到 Internet 的路由，则此设置为最佳设置。确保在网关路由器上为Catalyst 3850可以到达的子网配置静态路由（最好是总结路由）。因为此配置不使用路由协议，所以此步骤非常重要。
- 如果您的网络中有两台Catalyst 3850交换机，则可以将接入层交换机双连接到3850交换机，然后在交换机之间运行热备份路由器协议(HSRP)，以便在网络中提供冗余。
- 如果您需要上行链路端口的额外带宽，则可以配置EtherChannel。在链路发生故障时，EtherChannel还提供链路冗余。

配置

本文档使用以下配置：

- Catalyst 3850
- Catalyst 4500-A
- Catalyst 4500-B

Catalyst 3850

```
<#root>

SW_3850#

show running-config

Building configuration...

Current configuration : 11543 bytes
!
! Last configuration change at 12:16:54 UTC Tue Nov 15 2022
!
version 16.12
```

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service internal
service call-home
no platform punt-keepalive disable-kernel-core
!
hostname SW_3850

!
!--- IP routing enabled for Inter VLAN routing.



ip routing

!
!
no ip domain lookup
!
!
login on-success log
!
!
!

vtp mode off


!
!--- Output suppressed.

!--- Configure IEEE 802.1q trunks.
!--- Issue the switchport mode trunk command to force the switch port to trunk mode.
!--- Note: The default trunking mode is dynamic auto. If you establish a trunk link
!--- with the default trunking mode, the trunk does not appear
!--- in the configuration, even though a trunk has been established on
!--- the interface. Use the show interfaces trunk command to verify the
!--- establishment of the trunk.

!
interface GigabitEthernet1/0/1
 shutdown
!
interface GigabitEthernet1/0/2
 shutdown
!

interface GigabitEthernet1/0/3
 description To_Switch-B
 switchport mode trunk

!
interface GigabitEthernet1/0/4
 no switchport
 no ip address
 shutdown
!

interface GigabitEthernet1/0/5
```

```
 description To_Switch-A


 switchport mode trunk


!
interface GigabitEthernet1/0/6
no switchport
no ip address
shutdown
!
interface Vlan1
 no ip address
 shutdown
!

!--- This SVI (Switch Virtual Interface) is the default gateway for Users.
!
interface Vlan2


 description User-SVI


 ip address 10.1.2.1 255.255.255.0


!

!--- This SVI is the default gateway for Servers.
!
interface Vlan3


 description Server-SVI


 ip address 10.1.3.1 255.255.255.0


!

!--- This SVI is the default gateway for other L2 switches management interface.
!
interface Vlan10


 description Management-SVI


 ip address 10.1.10.1 255.255.255.0


!

!--- This route statement allows the 3850 to send Internet traffic to the Cisco router.
```

```
ip route 0.0.0.0 0.0.0.0 10.1.1.2


ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
!
!
line con 0
line vty 5 15
!
end
```

注意：在本示例中，所有交换机上的VLAN中继协议(VTP)均设置为off。此交换机使用以下命令将VTP设置为off并创建用户从全局配置模式定义的三个VLAN:

```
<#root>

SW_3850(config)#

vtp mode off

Setting device to VTP Off mode for VLANS.
SW_3850(config)#

vlan 2

SW_3850(config-vlan)#

name User_VLAN

SW_3850(config-vlan)#

exit

SW_3850(config)#

vlan 3

SW_3850(config-vlan)#

name Server_VLAN

SW_3850(config-vlan)#

exit

SW_3850(config)#

vlan 10

SW_3850(config-vlan)#

name Mgmt_VLAN

SW_3850(config-vlan)#

exit
```

```
SW_3850(config)#
end
```

Catalyst 4500-A

<#root>

Switch-A#

show running-config

```
Building configuration...

Current configuration : 15360 bytes
!
! Last configuration change at 01:06:17 UTC Wed Nov 16 2022
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service compress-config
!
```

hostname Switch-A

```
!
no ip domain-lookup
no ip dhcp snooping information option
!
!
login block-for 60 attempts 3 within 60
login delay 1
login quiet-mode access-class testblock
login on-failure log
login on-success log
```

vtp mode off

```
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!


vlan 3
 name Server-VLAN
!
vlan 10
 name Mgmt-VLAN

!

!--- Output suppressed

!
```

```
interface GigabitEthernet1/1
 shutdown
!
interface GigabitEthernet1/2
 shutdown
!
interface GigabitEthernet1/3
 switchport mode trunk

!

!--- Configure Server (Host-A) to be the on the access VLAN 3.

!

interface TenGigabitEthernet3/1
 switchport access vlan 3
 switchport mode access

!
interface TenGigabitEthernet3/2
 shutdown
!
interface TenGigabitEthernet3/3
!
interface TenGigabitEthernet3/4
!

!--- Output suppressed.
!--- IP address on VLAN 10 manages this switch.

!
interface Vlan1
 no ip address
!
interface Vlan10
 ip address 10.1.10.2 255.255.255.0

!
ip forward-protocol nd
ip http server
ip http banner
ip http authentication local
!

!--- Configure the default gateway so that the switch is reachable from other
!--- VLANs/subnets. The gateway points to the VLAN 10 interface on the 3850.

ip default-gateway 10.1.10.1
ip forward-protocol nd
ip http server
ip http banner
ip http authentication local
!
!
line con 0
 stopbits 1
line vty 0 4
 logging synchronous
 transport input all
```

```
line vty 5 15
 logging synchronous
 transport input all
!
end
```

Catalyst 4500-B

<#root>

Switch-B#

show running-config

```
Building configuration...

Current configuration : 6841 bytes
!
! Last configuration change at 10:44:33 UTC Tue Nov 15 2022
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
```

hostname Switch-B

```
!
boot-start-marker
boot system bootflash:cat4500es8-universal.SPA.03.11.06.E.152-7.E6.bin
boot-end-marker
!
!
vrf definition mgmtVrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
no aaa new-model
hw-module module 7 mode 1
!
!
!
!
!
!
!
!
!
!
```

vtp mode off

```
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan 2
name User-VLAN
!
vlan 10 name
Mgmt-VLAN


!
!
interface GigabitEthernet1/1
 switchport mode trunk

!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
 shutdown
!
interface GigabitEthernet1/4
 shutdown
!

!--- Output suppressed.
!--- Configure User (Host-B) in VLAN 2.

!
interface GigabitEthernet8/5
 switchport access vlan 2
 switchport mode access

!

!--- Configure the management IP address in VLAN 10.

!
interface Vlan1
 no ip address
!
interface Vlan10
 ip address 10.1.10.3 255.255.255.0

!

!--- Define the default route so that the switch is reachable.

!

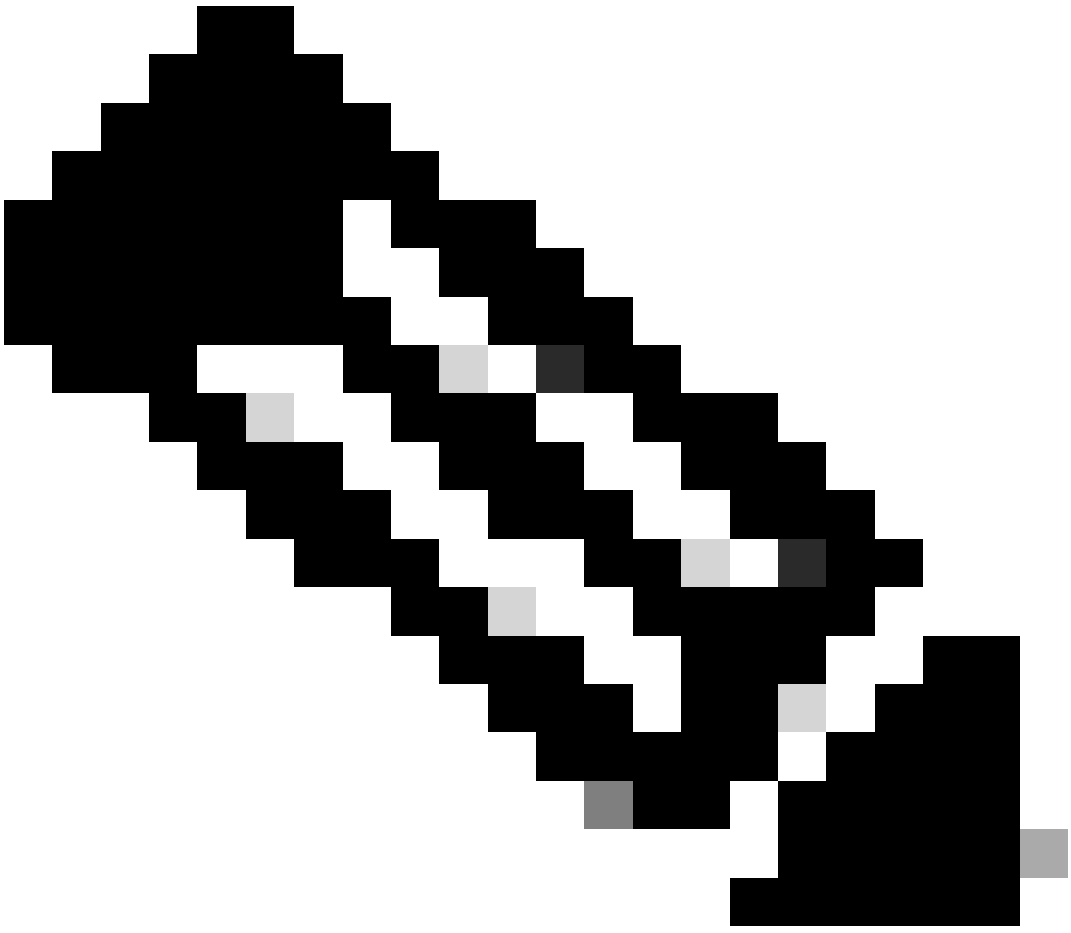

ip default-gateway 10.1.10.1


ip forward-protocol nd
ip http server
ip http banner
```

```
ip http authentication local
!
!
line con 0
 stopbits 1
line vty 0 4
 login
 transport input none
!
!
end
```

验证

本部分提供的信息可帮助您确认您的配置是否可正常运行。



注意：Cisco CLI Analyzer工具可帮助排除故障并检查此使用集成TAC工具和知识的智能SSH客户端支持的思科软件的整体运行状况。

注意：有关CLI命令的详细信息，请参阅特定交换平台的命令参考指南。

注意：只有注册思科用户才能访问此类工具和其他内部信息。

Catalyst 3850

- show vtp status

<#root>

SW_3850#

show vtp status

```
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : bc67.1c5d.3800
Configuration last modified by 10.0.0.10 at 0-0-00 00:00:00

Feature VLAN:
--------------
```

VTP Operating Mode   : Off

```
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 8
Configuration Revision            : 0
MD5 digest                        : 0x7E 0xC3 0x8D 0x91 0xC8 0x53 0x42 0x14
                                    0x79 0xA2 0xDF 0xE9 0xC0 0x06 0x1D 0x7D
```

- show interfaces trunk

<#root>

SW_3850#

show interfaces trunk

```
Port        Mode             Encapsulation  Status        Native vlan
```

Gi1/0/3   on   802.1q   trunking   1
Gi1/0/5   on   802.1q   trunking   1

```
Port        Vlans allowed on trunk
```

Gi1/0/3   1-4094
Gi1/0/5   1-4094

```
Port        Vlans allowed and active in management domain

Gi1/0/3     1-3,10
Gi1/0/5     1-3,10

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/3     1-3,10
Gi1/0/5     1,3,10
```

- show ip route

<#root>

SW_3850#

show ip route

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 10.100.100.2 to network 0.0.0.0


S*    0.0.0.0/0 [1/0] via 10.100.100.2

      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C        10.1.2.0/24 is directly connected, Vlan2
L        10.1.2.1/32 is directly connected, Vlan2
C        10.1.3.0/24 is directly connected, Vlan3
L        10.1.3.1/32 is directly connected, Vlan3
C        10.1.10.0/24 is directly connected, Vlan10
L        10.1.10.1/32 is directly connected, Vlan10
C        10.100.100.0/24 is directly connected, GigabitEthernet1/0/2
L        10.100.100.1/32 is directly connected, GigabitEthernet1/0/2
```

Catalyst 4500-A

- show vtp status

<#root>

Switch-A#

show vtp status

```
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : cisco.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 6400.f13e.dc40
Configuration last modified by 10.1.10.2 at 0-0-00 00:00:00

Feature VLAN:
--------------

VTP Operating Mode              : Off

Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 32
Configuration Revision            : 0
MD5 digest                        : 0x0B 0x61 0x4F 0x9B 0xCD 0x1B 0x37 0x55
                                    0xAB 0x0C 0xC1 0x4B 0xF8 0xDE 0x33 0xB3
```

- show interfaces trunk

<#root>

Switch-A#

show interfaces trunk

```
Port        Mode             Encapsulation  Status        Native vlan
Gi1/3       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi1/3       1-4094

Port        Vlans allowed and active in management domain
Gi1/3       1,3,10

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/3       1,3,10
```

Catalyst 4500-B

- show vtp status

<#root>

Switch-B#

show vtp status

```
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 6c20.5606.3540
Configuration last modified by 10.1.10.3 at 11-15-22 10:42:29

Feature VLAN:
--------------

VTP Operating Mode              : Off

Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 7
Configuration Revision            : 0
MD5 digest                        : 0xEC 0xB4 0x8D 0x46 0x94 0x95 0xE0 0x8F
                                    0xEE 0x1E 0xC7 0x9F 0x26 0x88 0x49 0x9F
```

- show interfaces trunk

<#root>

Switch-B#

show interfaces trunk

```
Port        Mode             Encapsulation  Status        Native vlan
Gi1/1       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi1/1       1-4094

Port        Vlans allowed and active in management domain
Gi1/1       1-2,10

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/1       1-2,10
```

故障排除

使用本部分可排除配置故障。

故障排除步骤

请使用以下说明：

1. 如果无法对同一 VLAN 内的设备执行 ping 操作，请检查源端口及目标端口的 VLAN 分配，确保源和目标在同一 VLAN 内。

   要检查VLAN分配，请对Cisco IOS软件发出 show interface status命令。

   如果源设备和目的设备不在同一台交换机中，请确保您已正确配置中继。要检查配置，请发出show interfaces trunk命令。

2. 此外，检查中继链路两端的本征VLAN是否匹配。确保源设备及目标设备之间的子网掩码相匹配。

3. 如果无法对不同 VLAN 中的设备执行 ping 操作，请确保能够对各自的默认网关执行 ping 操作。（请参阅步骤1。）

   此外，请确保设备的默认网关指向正确的 VLAN 接口 IP 地址。确保子网掩码匹配。

4. 如果无法连接 Internet，请确保 3850 上的默认路由指向正确的 IP 地址，并且子网地址与 Internet 网关路由器匹配。

   要检查，请发出show ip interface interface-id命令。确保 Internet 网关路由器有指向 Internet 和内部网络的路由。

相关信息

- 在 Catalyst 交换机上创建以太网 VLAN
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。