



Table of Contents

CCIE Routing & Switching

▶ Unit 1: Preparation

▼ Unit 2: Switching

Static MAC Address Table Entry

Cisco Switch Virtualization

Introduction to VLANs (Virtual LAN)

How to configure VLANs

802.1Q Encapsulation

How to configure a trunk between switches

Cisco DTP (Dynamic Trunking Protocol) Negotiation

802.1Q Tunneling (Q-in-Q)

Etherchannel over 802.1Q Tunneling

How to change the Native VLAN

VTP (VLAN Trunking Protocol)

VTP Version 3

Protected Port

Private VLANs (PVLAN)

Introduction to Spanning-Tree

Spanning-Tree Cost Calculation

PVST (Per VLAN Spanning Tree)

Spanning-Tree Port States

Spanning-Tree TCN (Topology Change Notification)

Spanning-Tree Portfast

Spanning-Tree UplinkFast

[Spanning-Tree Backbone Fast](#)
[Rapid Spanning-Tree](#)
[Rapid Spanning-Tree Configuration](#)
[MST \(Multiple Spanning-Tree\)](#)
[Spanning-Tree BPDUGuard](#)
[Spanning-Tree BPDUFilter](#)
[Spanning-Tree RootGuard](#)
[Spanning-Tree LoopGuard and UDLD](#)
[FlexLinks](#)
[Introduction to Etherchannel](#)
[Layer 3 Etherchannel](#)
[Cisco IOS SPAN and RSPAN](#)

- ▶ [Unit 3: IP Routing](#)
- ▶ [Unit 4: RIP](#)
- ▶ [Unit 5: EIGRP](#)
- ▶ [Unit 6: OSPF](#)
- ▶ [Unit 7: BGP](#)
- ▶ [Unit 8: Multicast](#)
- ▶ [Unit 9: IPv6](#)
- ▶ [Unit 10: Quality of Service](#)
- ▶ [Unit 11: Security](#)
- ▶ [Unit 12: System Management](#)
- ▶ [Unit 13: Network Services](#)
- ▶ [Unit 14: MPLS](#)

You are here: [Home](#) » [Cisco](#) » [CCIE Routing & Switching](#)

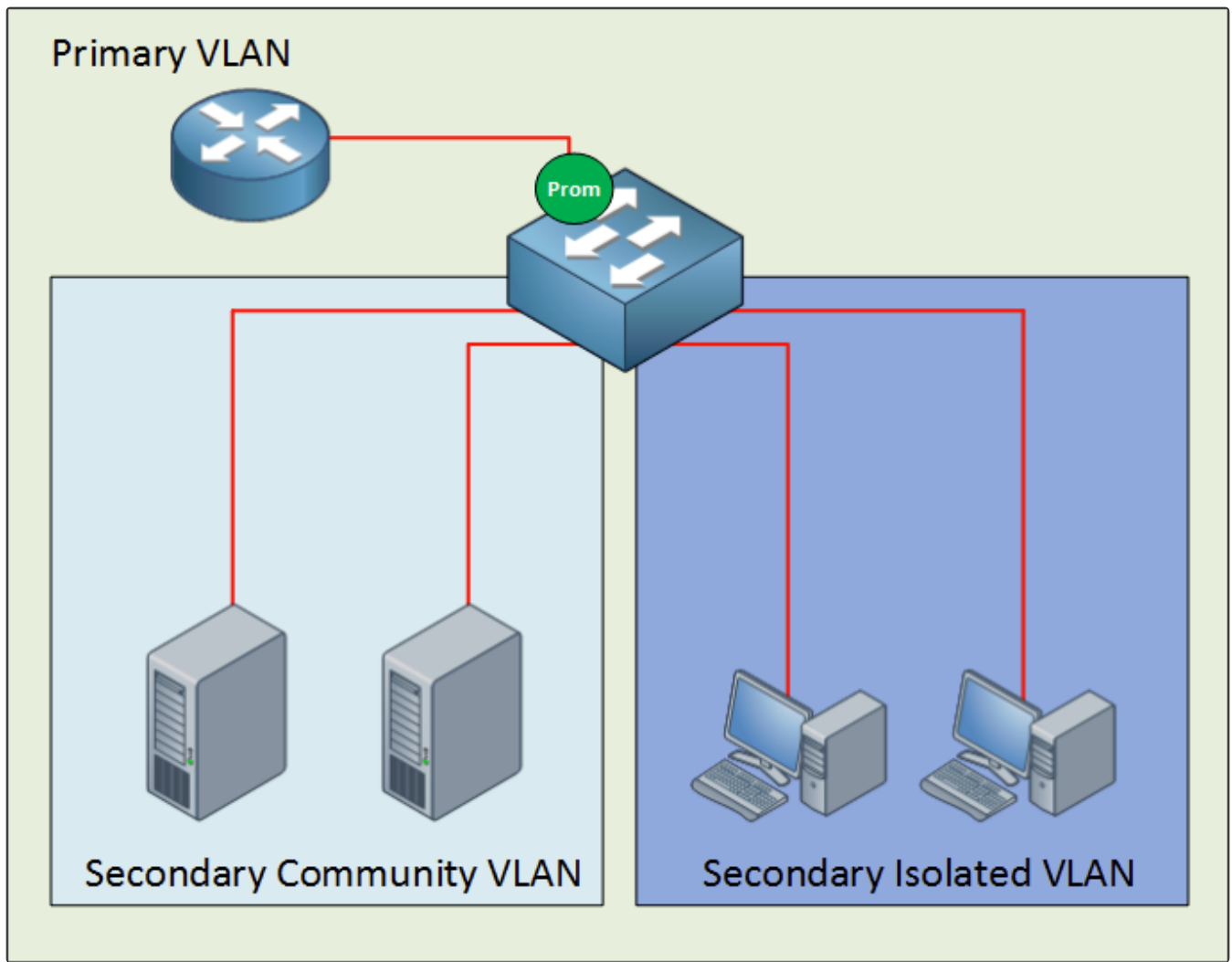
Private VLAN (PVLAN) on Cisco Catalyst Switch



13 votes



In a previous tutorial I explained the [protected port](#) feature on Cisco Catalyst Switches. This time we will look at the private VLAN which I can best describe as *protected ports on steroids*. If you have no idea what a protected port or VLAN is, I highly recommend to read my [previous tutorial](#) first. Having said that, let's get started with a nice topology picture:



Many network students believe private VLANs are very complex when they see this for the first time. I'm going to break it down and explain to you how it works.

The private VLAN always has **one primary VLAN**. Within the primary VLAN you will find the promiscuous port. In my picture above you can see that there's a router connected to a promiscuous port. **All other ports are able to communicate with the promiscuous port.** Within the primary VLAN you will encounter one or more secondary VLANs, there are two types:

- **Community VLAN:** All ports within the community VLAN are **able** to communicate with each other and the promiscuous port.
- **Isolated VLAN:** All ports within the isolated VLAN are **unable** to communicate with each other but they can communicate with the promiscuous port.

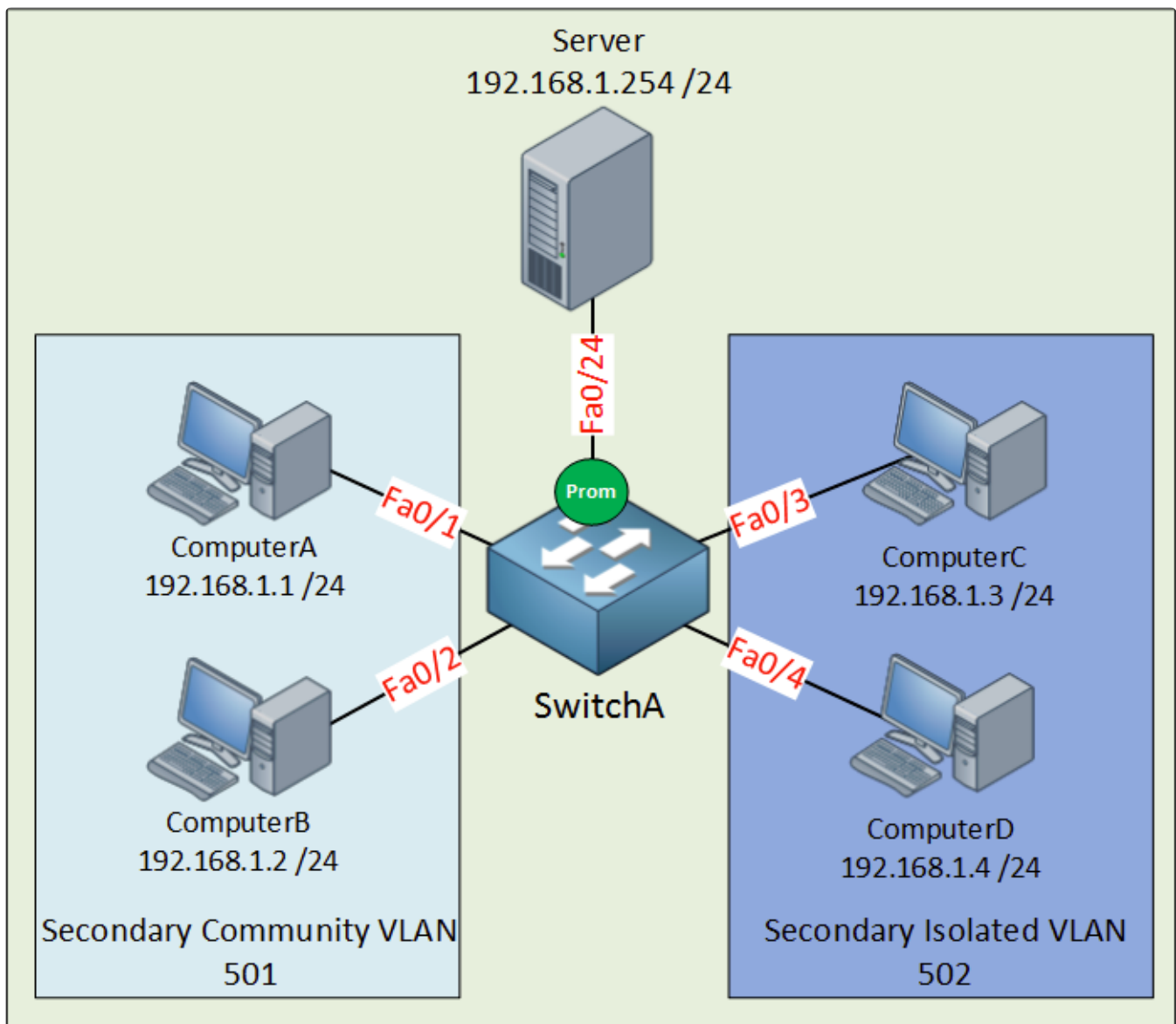


The names for these secondary VLANs are well chosen if you ask me. In a community everyone is able to talk to each other. When you are isolated you can only talk to yourself or in case of our private VLANs... the promiscuous port.

Secondary VLANS can always communicate with the promiscuous port but they can **never communicate with other secondary VLANs!** Are you following me so far? If so...good! If you are still a little fuzzy, don't worry. I'm going to show you the configuration and demonstrate to you how this works.

Configuration

First let me show you the topology that I will use for this demonstration:



Let me sum up what we have here:

- The primary VLAN has number 500.
- The secondary community VLAN has number 501.
- The secondary isolated VLAN has number 502.
- I just made up these VLAN numbers; you can use whatever you like.

- ComputerA and ComputerB in the community VLAN should be able to reach each other and also the server connected to the promiscuous port.
- ComputerC and ComputerD in the isolated VLAN can only communicate with the server on the promiscuous port.
- The server should be able to reach all ports.

Let's get started!

```
SwitchA(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
```

Configuring private VLANs requires us to change the VTP mode to Transparent.

```
SwitchA(config)#vlan 501
SwitchA(config-vlan)#private-vlan community
SwitchA(config-vlan)#vlan 500
SwitchA(config-vlan)#private-vlan primary
SwitchA(config-vlan)#private-vlan association add 501
```

Let's start with the configuration of the community VLAN. First I create VLAN 501 and tell the switch that this is a community VLAN by typing the **private-vlan community** command. Secondly I am creating VLAN 500 and configuring it as the primary VLAN with the **private-vlan primary** command. Last but not least I need to tell the switch that VLAN 501 is a secondary VLAN by using the **private-vlan association** command.

```
SwitchA(config)#interface range fa0/1 - 2
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 500 501
```

Interface fa0/1 and fa0/2 are connected to ComputerA and ComputerB and belong to the community VLAN 501. On the interface level I need to tell the switch that these are host ports by issuing the **switchport mode private-vlan host** command. I also have to use the **switchport private-vlan host-association** command to tell the switch that VLAN 500 is the primary VLAN and 501 is the secondary VLAN.

```
SwitchA(config)#interface fa0/24
SwitchA(config-if)#switchport mode private-vlan promiscuous
```

```
SwitchA(config-if)#switchport private-vlan mapping 500 501
```

This is how I configure the promiscuous port. First I have to tell the switch that fa0/24 is a promiscuous port by typing the switchport mode private-vlan promiscuous command. I also have to map the VLANs by using the switchport private-vlan mapping command. Here is the output for FastEthernet 0/1:

```
SwitchA#show interfaces fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 500 (VLAN0500) 501 (VLAN0501)
Administrative private-vlan mapping: none
```

We can verify our configuration by looking at the switchport information. Interface fa0/24 has the same configuration as fa0/1.

```
SwitchA#show interface fa0/24 switchport
Name: Fa0/24
Switchport: Enabled
Administrative Mode: private-vlan promiscuous
Operational Mode: private-vlan promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 500 (VLAN0500) 501 (VLAN0501)
```

Here is the switchport information for fa0/24 (our promiscuous port). You can see the mapping information.

```
SwitchA#show vlan private-vlan
Primary Secondary Type Ports
-----
-
500 501 community Fa0/1, Fa0/2, Fa0/24
```

The show vlan private-vlan command gives us valuable information. You can see that VLAN 500 is the primary VLAN and 501 is the secondary VLAN. It also tells us whether the VLAN is a community or isolated VLAN the ports.

```
SwitchA#show vlan private-vlan type
Vlan Type
----
500 primary
501 community
```

I also like the **show vlan private-vlan type** command because it gives us a quick overview of the private VLANs.

So what's the result of this configuration?

If everything is OK we should now have a working community VLAN...let's find out!

```
C:\Documents and Settings\ComputerA>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
```

ComputerA is able to reach ComputerB.

```
C:\Documents and Settings\ComputerA>ping 192.168.1.254
Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time<1ms TTL=128
```

ComputerA can also reach the server behind the promiscuous port.

```
C:\Documents and Settings\Server>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
```

The server is able to reach ComputerB. Great! Our community VLAN seems to be up and running. Let's continue with the configuration of the isolated VLAN.

```
SwitchA(config)#vlan 502
SwitchA(config-vlan)#private-vlan isolated
SwitchA(config-vlan)#vlan 500
SwitchA(config-vlan)#private-vlan primary
SwitchA(config-vlan)#private-vlan association add 502
```

The configuration is the same as the community VLAN but this time I'm using the **private vlan isolated** command. Don't forget to add the association between the primary and secondary VLAN using the private-vlan association add command. The private-vlan primary command is obsolete because I already did this before, I'm just showing it to keep the configuration complete.

```
SwitchA(config)#interface range fa0/3 - 4
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 500 502
```

This part is exactly the same as the configuration for the community VLAN but I'm configuring interface fa0/3 and fa0/4 which are connected to ComputerC and ComputerD.

```
SwitchA(config)#interface fa0/24
SwitchA(config-if)#switchport mode private-vlan promiscuous
SwitchA(config-if)#switchport private-vlan mapping 500 502
```

I already configured fa0/24 as a promiscuous port but I'm showing it here as well to keep the configuration complete. I do need to create an additional mapping between VLAN 500 (primary) and VLAN 502 (secondary).

Let's verify our work!


```
SwitchA#show interfaces fa0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 500 (VLAN0500) 502 (VLAN0502)
Administrative private-vlan mapping: none
```

Looking good...we can see the host-association between VLAN 500 and 502.

```
SwitchA#show interfaces fastEthernet 0/4 switchport | include host-as
Administrative private-vlan host-association: 500 (VLAN0500) 502 (VLAN0502)
```

A quick look at fa0/4 shows me the same output as fa0/3.

```
SwitchA#show interfaces fa0/24 switchport
Name: Fa0/24
Switchport: Enabled
Administrative Mode: private-vlan promiscuous
Operational Mode: private-vlan promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 500 (VLAN0500) 501 (VLAN0501) 502 (VLAN0502)
```

We can now see that VLAN 501 and VLAN 502 are mapped to primary VLAN 500.

```
SwitchA#show vlan private-vlan
```

```
Primary Secondary Type Ports
```

```
-----
```

```
-
```

```
500 501 community Fa0/1, Fa0/2, Fa0/24
```

```
500 502 isolated Fa0/3, Fa0/4, Fa0/24
```

Here's a nice clean overview which shows us all the VLANs, the mappings and the interfaces.

```
SwitchA#show vlan private-vlan type
```

```
Vlan Type
```

```
----
```

```
500 primary
```

```
501 community
```

```
502 isolated
```

Or if you only care about the VLAN numbers and the VLAN type this is what you need.

What will the result be of our hard labor?

```
C:\Documents and Settings\ComputerC>ping 192.168.1.254
```

```
Pinging 192.168.1.254 with 32 bytes of data:
```

```
Reply from 192.168.1.254: bytes=32 time<1ms TTL=128
```

ComputerC can reach the server behind the promiscuous port.

```
C:\Documents and Settings\ComputerD>ping 192.168.1.254
```

```
Pinging 192.168.1.254 with 32 bytes of data:
```

```
Reply from 192.168.1.254: bytes=32 time<1ms TTL=128
```

ComputerD can also reach the server behind the promiscuous port.

```
C:\Documents and Settings\ComputerC>ping 192.168.1.4
```

```
Pinging 192.168.1.4 with 32 bytes of data:
```

```
Request timed out.  
Ping statistics for 192.168.1.4:  
Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
```

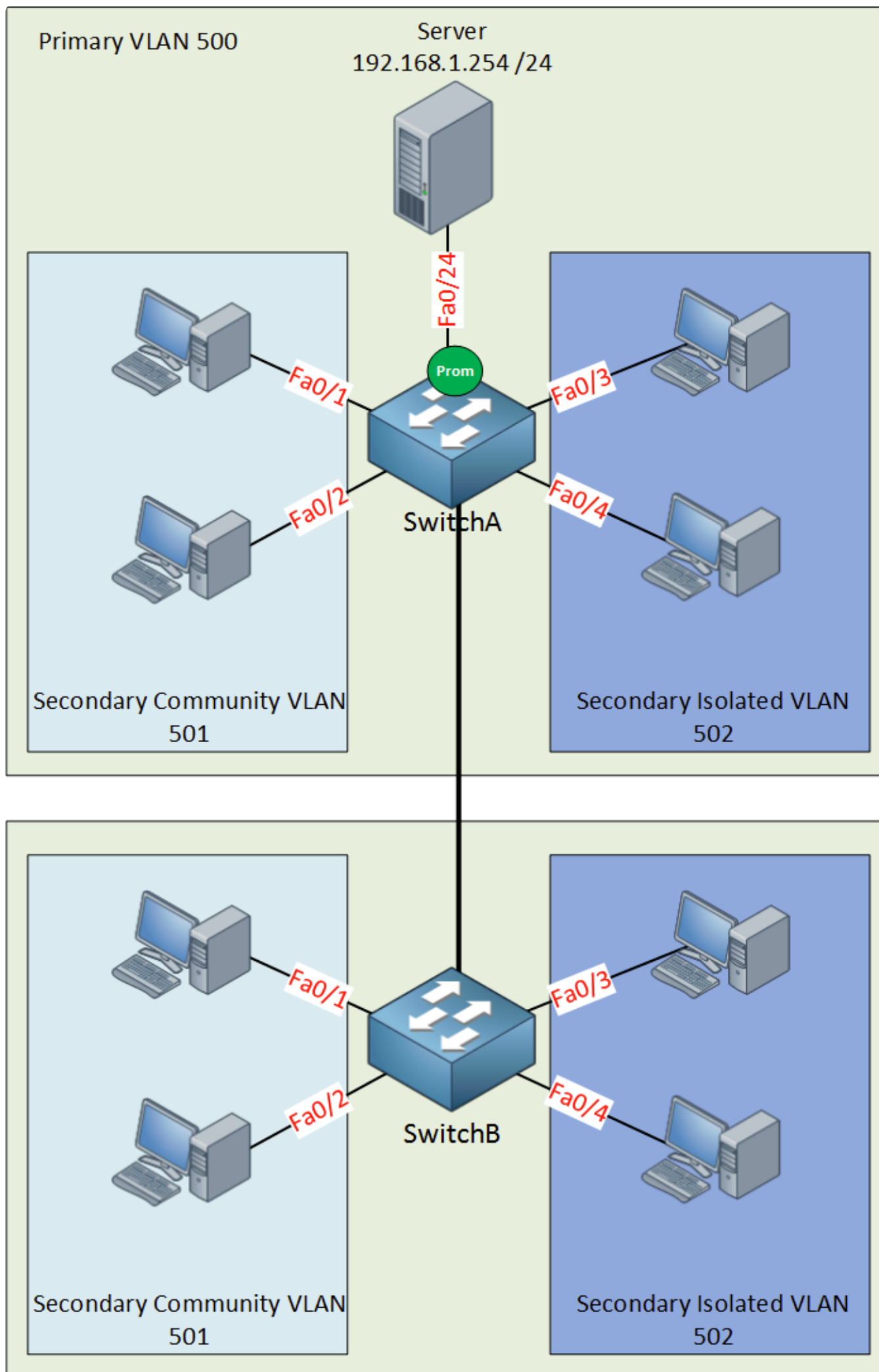
There is no reachability between ComputerC and ComputerD because they are in the isolated VLAN.

What about reachability between VLAN 501 and VLAN 502? Let's give it a try:

```
C:\Documents and Settings\ComputerA>ping 192.168.1.4  
Pinging 192.168.1.4 with 32 bytes of data:  
Request timed out.  
Ping statistics for 192.168.1.4:  
Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
```

This is ComputerA in VLAN 501 trying to reach ComputerD in VLAN 502. As you can see this isn't possible. You are unable to communicate between different secondary VLANs.

That's all I have for now about the configuration, anything else you need to know about private VLANs?



Private VLANs can be carried over 802.1Q links so it's possible to span your configuration over multiple switches. In the picture above I expanded our configuration to SwitchB. The configuration on SwitchB will be the same as SwitchA. You just need to make sure that VLAN 500, 501 and 502 can be carried over the trunk between SwitchA and SwitchB. Don't forget that because of VTP transparent mode, VLAN information is not synchronized between the two switches. You'll have to create the VLANs yourself on the other switches.

Let me give you a short overview of what you have learned by now:

- Devices within a community VLAN can communicate with each other AND the promiscuous port.
- Devices within an isolated VLAN cannot communicate with each other and can ONLY communicate with the promiscuous port.
- The promiscuous port can communicate with any other port.
- Secondary VLANs are unable to communicate with other secondary VLANs.
- Private VLANs can be spanned across multiple switches if you use trunks.



That's all I have for you about private VLANs! What do you think? I hope this all makes sense to you.


Rate this Lesson:



« [Previous Lesson](#)
[Protected Port](#)

[Next Lesson](#) »
[Introduction to Spanning-Tree](#)

[Home](#) › [Forums](#) › Private VLAN (PVLAN) on Cisco Catalyst Switch

This topic contains 47 replies, has 19 voices, and was last updated by  Andrew P [3 days, 10 hours ago](#).

Viewing 15 posts - 1 through 15 (of 47 total)

1 2 ... 4 →

- Author
Posts | [Subscribe](#)
- April 10, 2015 at 10:52 [#11858 Reply](#)



Edwin P
Participant
Hi Rene,

I trying to lab this up but how exactly to did you configure the trunk port between the 2 switches as a promiscuous port?
switchport mode is then promiscuous..not trunk..or am i missing something?
I am talking about the private-vlans across 2 switches (the last diagram here)

Thanks

Edwin



April 10, 2015 at 10:59 [#11859 Reply](#)



Rene Molenaar
Keymaster
Hi Edwin,

I think I left the “prom” icon on SwitchB there by accident, you don’t have to do anything special with the trunk. Just a regular 802.1q trunk between SwitchA + SwitchB is what you need to get this working.

Let me know if that works ok? I’ll fix the picture and if required I can create a configuration example for this.

Rene

April 12, 2015 at 16:10 [#11860 Reply](#)



Rene Molenaar
Keymaster
Just updated the picture.

April 22, 2015 at 20:55 #11861 Reply



Edwin P
Participant
Hi Rene,

It worksyes , i have found out that a switch that does not support private vlans natively (like the 3550) can actually also serve as “passthrough” as long as the community,isolated and primary vlan are created on it, the passthrough switch is then off course not intended to have any workstations configured in those vlans as they would not be able to communicate with the promisscuuous port anyhow..interesting.

thanks for your great article!

April 22, 2015 at 21:09 #11862 Reply



Edwin P
Participant
PS: What program do you use to draw these layouts?



April 22, 2015 at 21:41 #11863 Reply



Rene Molenaar
Keymaster
It's all done in Visio and the VisioCafe stencils:

<http://www.visiocafe.com/vsdfx.htm>

June 20, 2015 at 14:18 #11864 Reply



Srinivasan C
Participant
Hi Rene,

I doest not want to give access to some of my servers for some hosts in isolated community.
Can I configure some servers and some hosts in isolated community as protected ports

while allowing other hosts in isolated community to access servers ?
Does it work with private-vlan?

Thanks ,
Srini

June 25, 2015 at 16:32 [#11865 Reply](#)



Rene Molenaar
Keymaster
Hi Srini,

I think you are better off with creating some access-lists for this. If you use an isolated VLAN then all devices within the isolated VLAN will be unable to talk with each other. It's used for separation within the VLAN.

For your hosts, it's probably easier to create two regular VLANs for your hosts and one (or more) VLAN(s) for your servers. Use access-lists to permit/deny traffic between these different VLANs.



Rene

October 5, 2015 at 11:14 [#17753 Reply](#)



Siva S
Participant
Hi Rene,

Regarding this statement : "Secondary VLANs are unable to communicate with other secondary VLANs."

Based on your first example on top, let's say if :

Computer A and B are inside Secondary Community Vlan 501

And Computer C and D are inside Secondary Community Vlan 502.

Am i right to say, Computer A and B won't be able to ping C and D?

Had to confirm this as I'm unable to test this on my emulator.

Thanks & Regards,

Siva

October 5, 2015 at 12:35 [#17756 Reply](#)



Rene Molenaar
Keymaster
Hi Siva,

That's right, there is no communication between these two secondary VLANs.

Rene



October 11, 2015 at 08:49 [#17971 Reply](#)



Frades
Participant
Great lessons rene! easy to understand!

my question is, how can i simulate this one? especially the computers and servers?

my plan is to purchase the normal lab which are:

2 x 2950

1 x 3560

i only have a laptop. no other computers around. is there any other way i can simulate the computers? thanks!

October 11, 2015 at 09:16 [#17972 Reply](#)



Frades

Participant

Followup question on Siva.

So secondary vlans cant talk with other secondary vlans. in short, community vlans cant talk with other community vlans that have a different VLAN? right?

Community 501 and Community 502 = users on 501 cant talk with 502 and vice versa right?

but what if you spanned the private vlans on trunk

Community 501 — Switch -(TRUNK)- Switch — Community 501

can the left side community 501 users can talk with the right side community 501 users?

October 11, 2015 at 09:21 [#17973 Reply](#)



Rene Molenaar

Keymaster

Hi John,



If you have no computers then you can also use switches, routers or USB NICs.

For example you could use the VLAN 1 interface on your 2950 switches to have something to ping with. Connect them to your 3560 with an interface in access mode VLAN 1 on the 2950 side.

Multiple cheap USB nics is also an option, you can use these to connect them to virtual machines on your computer.

You are correct about the secondary VLANs. One secondary VLAN can't talk with another secondary VLAN. Users in community VLAN 501 can only communicate with 501, not with 502.

Spanning a community VLAN over a trunk is no problem.

Rene

October 29, 2015 at 15:30 [#19314 Reply](#)



Jeppe A
Participant

If I understand this correct, then the hosts on Switch A VLAN 501 are able to communicate with the hosts on Switch B VLAN 501?

October 29, 2015 at 19:02 [#19323](#) [Reply](#)



Rene Molenaar
Keymaster

That's right, as long as VLAN 501 is a community VLAN.

- Author
Posts



Viewing 15 posts - 1 through 15 (of 47 total)

1 2 ... 4 →

Reply To: Private VLAN (PVLAN) on Cisco Catalyst Switch

b / link b-quote ↕ img ul ol li code close tags

Please put code in between `backticks` or use the CODE button.

To place inline images, please use any image share service (such as [TinyPic](#) or [Imgur](#)) and use the IMG button!

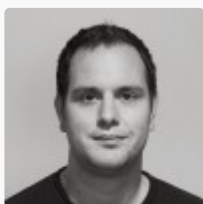
☐ Notify me of follow-up replies via email

Maximum file size allowed is 2048 KB.

Attachments:

 Файл не выбран[Add another file](#)

About NetworkLessons.com



Hello There! I'm René Molenaar (CCIE #41726), Your Personal Instructor of Networklessons.com. I'd like to teach you everything about Cisco, Wireless and Security. I am here to Help You Master Networking!



Social Fans



14,267

FANS



7,929

FOLLOWERS



1,589

SUBSCRIBERS

Highest Rated Lessons

MPLS Layer 3 VPN Configuration



(25 votes)

VRF Lite Configuration on Cisco IOS



(23 votes)

Cisco Portfast Configuration



(20 votes)

IPv6 Address Types



(18 votes)

EIGRP Stub Explained



(17 votes)

New Lessons

[Introduction to Cisco IOS XE](#)

[ERSPAN Configuration on Cisco IOS XE](#)

[IGMP Filter](#)

[IGMP Snooping without Router](#)

[Cisco Group Management Protocol \(CGMP\)](#)

[Disclaimer](#)

[Privacy Policy](#)

[Support](#)

Private VLAN (PVLAN) on Cisco Catalyst Switch written by Rene Molenaar average rating 4.8/5 - 13 user ratings

