



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](#)

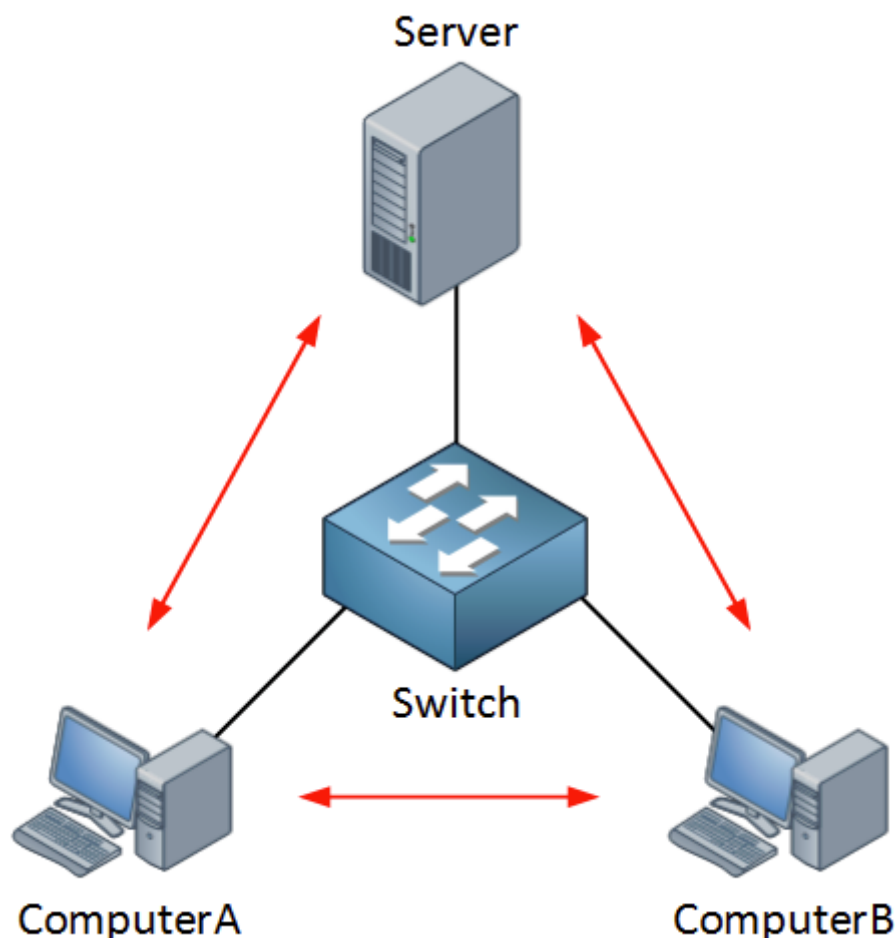
Protected Port on Cisco Catalyst Switch



12 votes



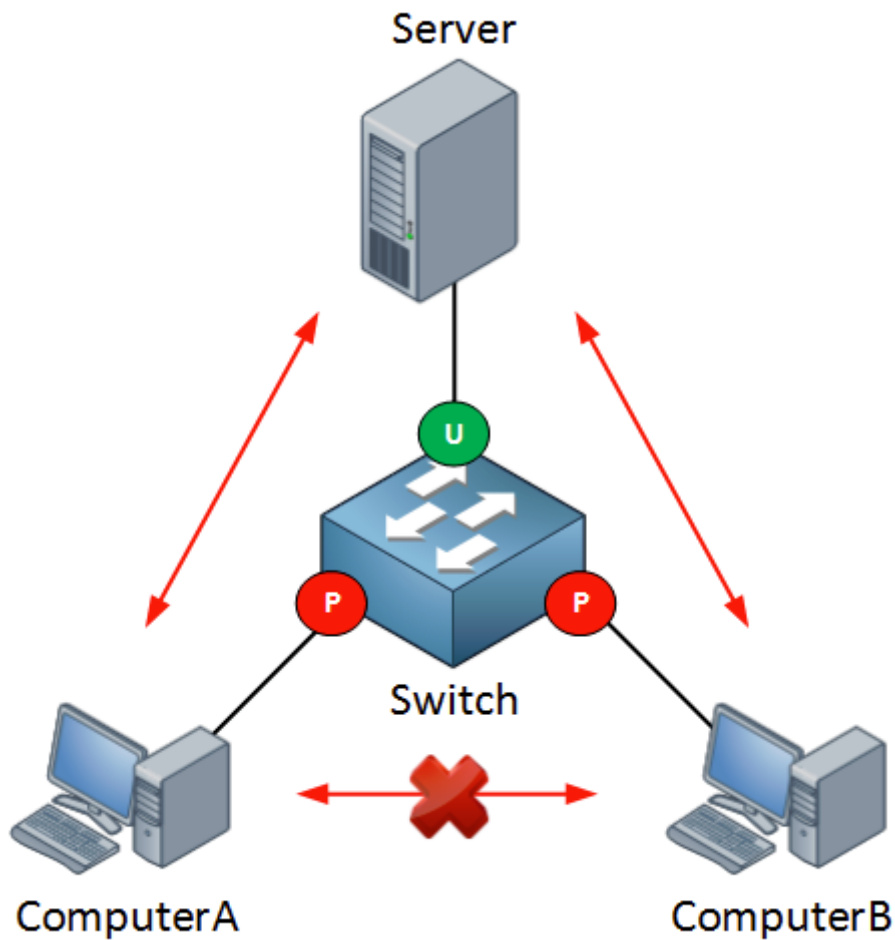
The protected port is a feature on Cisco Catalyst Switches that you can use to prevent interfaces from communicating with each other. Let me show you a picture to explain this:



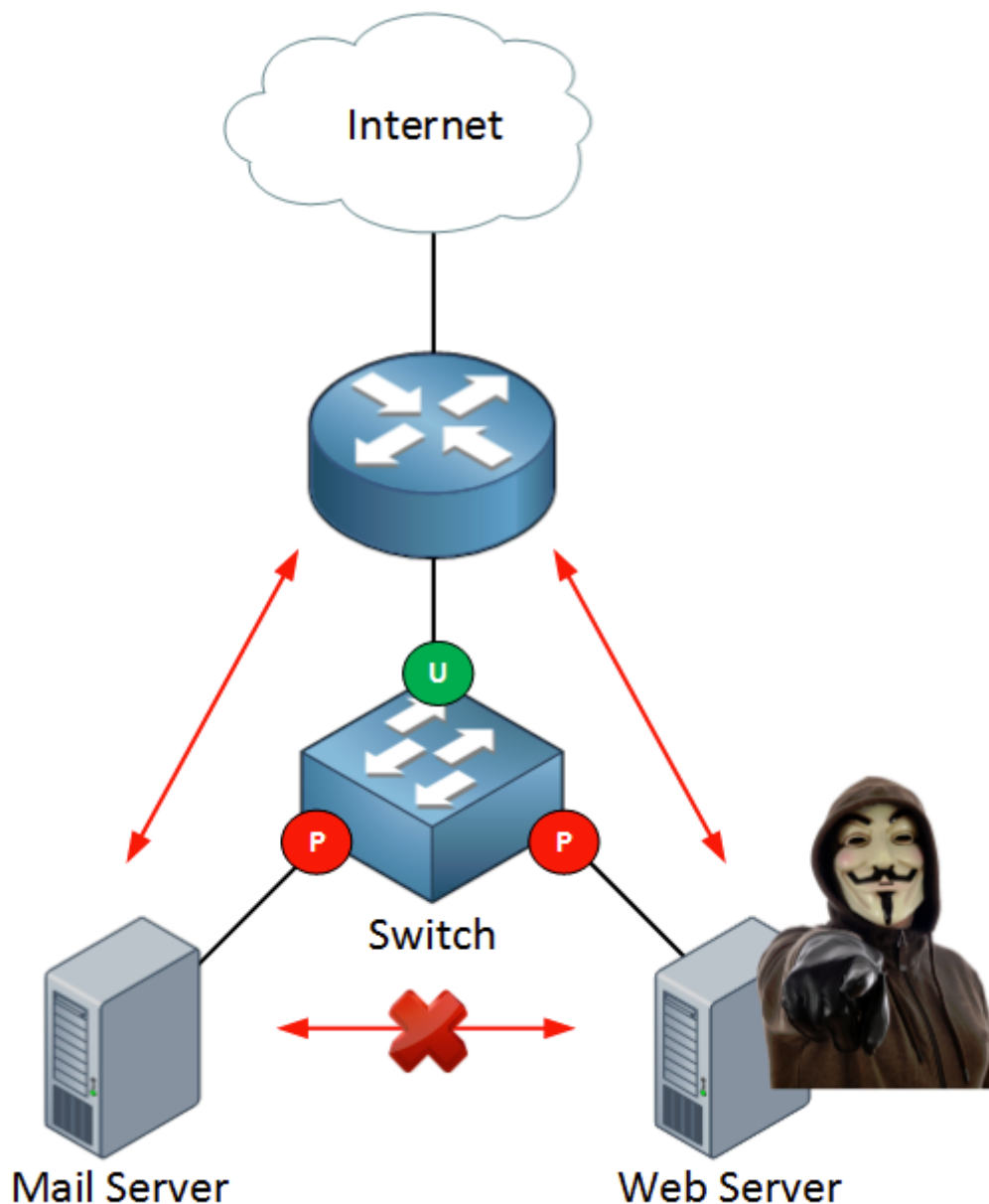
Take a look at the picture above. We have two computers, one switch and one server. Nothing fancy here...everything is in one VLAN and the two computers and server can communicate with each other.

What if I want to enhance security and ensure that ComputerA and ComputerB can only reach the server but not each other? This makes perfect sense in a client-server network. Normally there is no need for computers to connect to each other (unless Bob and Jane are secretly using shared folders on their computers without permission from the windows administrator).

We can ensure ComputerA and ComputerB are unable to communicate with each other by using **protected ports**. By default all switchports are unprotected. Here's what it looks like:



The interfaces connected to ComputerA and ComputerB are protected ports, the interface connected to the server is an unprotected port. **Protected ports are unable to communicate with each other.** It might also be a good idea to protect your servers with protected ports:



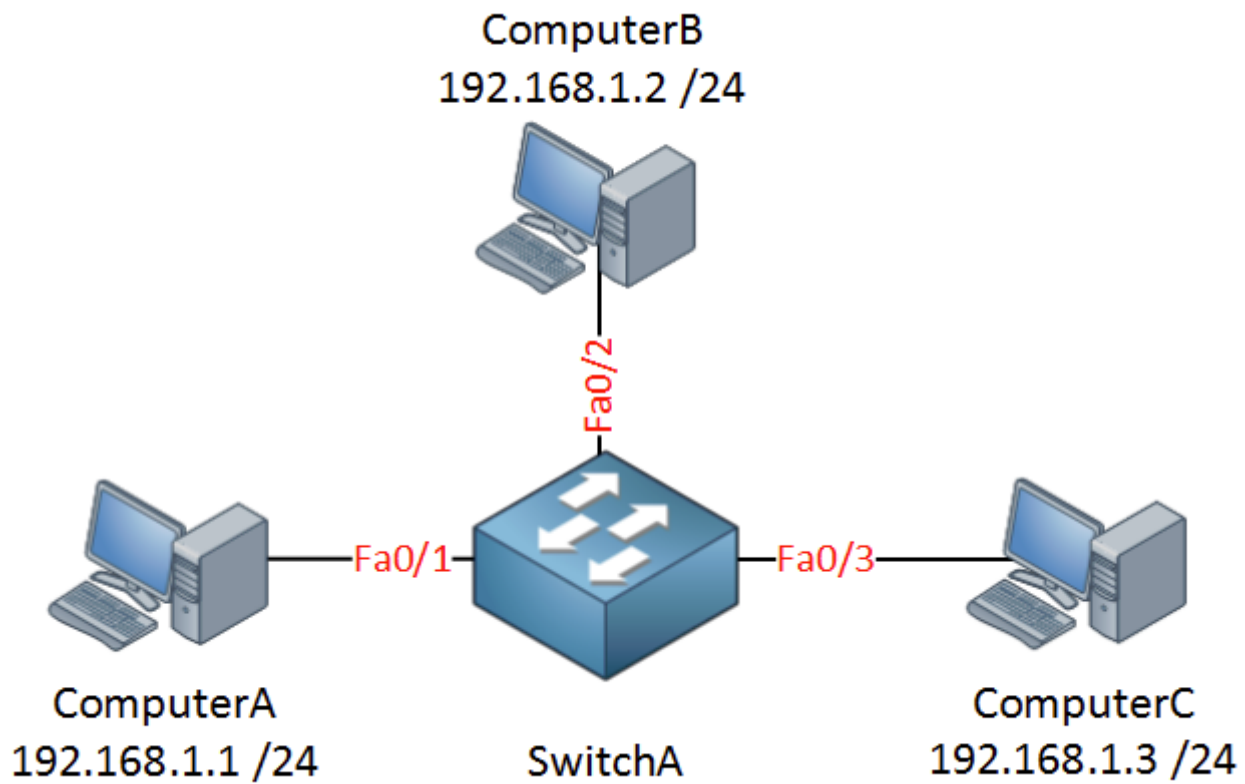
If a ~~freedom fighter~~ hacker takes over your web server you can reduce the attack surface by preventing them from connecting to other servers in your network.

This should give you an idea of what a protected port does, let's look at the actual configuration!

Configuration

To demonstrate this, we will use 3 computers connected to a single switch:

- All computers are in the same subnet (192.168.1.0 /24)
- All computers are in the same VLAN.
- Switch has a default configuration.



With the default configuration on the switch, alle computers are in the same VLAN so they can ping each other:

```
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
```

```
C:\Documents and Settings\ComputerA>ping 192.168.1.3
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
```

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

By sending a couple of pings we can verify that we have full reachability. Now I'm going to enable protected port on the interface connected to ComputerA and ComputerC:

```
SwitchA(config)#interface fa0/1
```

```
SwitchA(config-if)#switchport protected
```

```
SwitchA(config)#interface fa0/3
```

```
SwitchA(config-if)#switchport protected
```

The interfaces connected to ComputerA and ComputerC are now protected. Interface fa0/2 to ComputerB is still unprotected. You can verify this by looking at the output of the show switchport command:

```
SwitchB#show interfaces fa0/1 switchport
```

```
Name: Fa0/1
```

```
Switchport: Enabled
```

```
Administrative Mode: dynamic auto
```

```
Operational Mode: down
```

```
Administrative Trunking Encapsulation: negotiate
```

```
Negotiation of Trunking: On
```

```
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: none
```

```
Administrative private-vlan trunk native VLAN: none
```

```
Administrative private-vlan trunk Native VLAN tagging: enabled
```

```
Administrative private-vlan trunk encapsulation: dot1q
```

```
Administrative private-vlan trunk normal VLANs: none
```

```
Administrative private-vlan trunk associations: none
```

```
Administrative private-vlan trunk mappings: none
```

```
Operational private-vlan: none
```

```
Trunking VLANs Enabled: ALL
```

```
Pruning VLANs Enabled: 2-1001
```

```
Capture Mode Disabled
```

```
Capture VLANs Allowed: ALL
```

```
Protected: true
```

Let's send some more pings to find out what the result is of this configuration:

```
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
```

```
C:\Documents and Settings\ComputerC>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 and ComputerC are still able to reach ComputerB...

```
C:\Documents and Settings\ComputerA>ping 192.168.1.3
Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Ping statistics for 192.168.1.2:
Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
```

```
C:\Documents and Settings\ComputerC>ping 192.168.1.1
Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Ping statistics for 192.168.1.2:
Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
```

But ComputerA and ComputerC are unable to reach each other now.



Traffic between two protected ports is **blocked**, traffic between a protected and unprotected port is **allowed**.

The protected port feature is pretty cool but it is also very limited. In another tutorial I will show you how to configure Private VLANs which is basically the protected port on steroids.

Rate this Lesson:






« Previous Lesson
VTP Version 3

Next Lesson »
Private VLANs (PVLAN)

[Home](#) › [Forums](#) › Protected Port on Cisco Catalyst Switch

This topic contains 8 replies, has 7 voices, and was last updated by  Rene Molenaar 3 weeks, 6 days ago.

Viewing 8 posts - 1 through 8 (of 8 total)

- Author
Posts | [Subscribe](#)
- January 27, 2015 at 02:53 [#11867 Reply](#)



Kevin M
Member
protected port on steroids 😊

May 12, 2015 at 00:11 [#11868 Reply](#)



Mauro P
Participant
I also enjoyed the term 😊

August 7, 2015 at 07:48 [#11869 Reply](#)



Srinivasan C
Participant
Hi Reno,
Very Simple and Great explanation !

Regards,
Srini

October 10, 2015 at 14:55 [#17967 Reply](#)



Frades

Participant

lol freedom fighter.

lol protected port on steroids.

LOL! haha

December 7, 2015 at 06:27 [#20073 Reply](#)



SINAN A

Participant

Hello Rene,

Is the Protected option is available in Switch types like 2960 , 3560 ? if yes, i try to applied it on packet tracer which support both switch but it said not supported. Would you please let me know which switch is supported. Thank you

December 7, 2015 at 11:28 [#20074 Reply](#)



Rene Molenaar

Keymaster

Hi Sinan,

Yes it's available on the 2960 and 3560. I'm guessing that packet tracer doesn't support it, it's a simulator after all.

Rene

May 25, 2016 at 15:22 [#24464 Reply](#)



Mohammad Hasanuz Z

Participant

Hlw Rene,

this is good stuff, thanks. One questions

Protected port feature will work within SW local port & within Same VALN , right ??

br//

zaman



May 25, 2016 at 20:33 [#24468](#) [Reply](#)



Rene Molenaar

Keymaster

Hi Zaman,

That's right. It will work for the VLAN that the interface is assigned to.

Rene

- Author
Posts

Viewing 8 posts - 1 through 8 (of 8 total)

Reply To: Protected Port on Cisco Catalyst Switch



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!

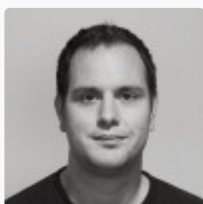
☐ Notify me of follow-up replies via email

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](#)

Protected Port on Cisco Catalyst Switch written by Rene Molenaar average rating 5/5 - 12 user ratings