Networklessons.com

Search...

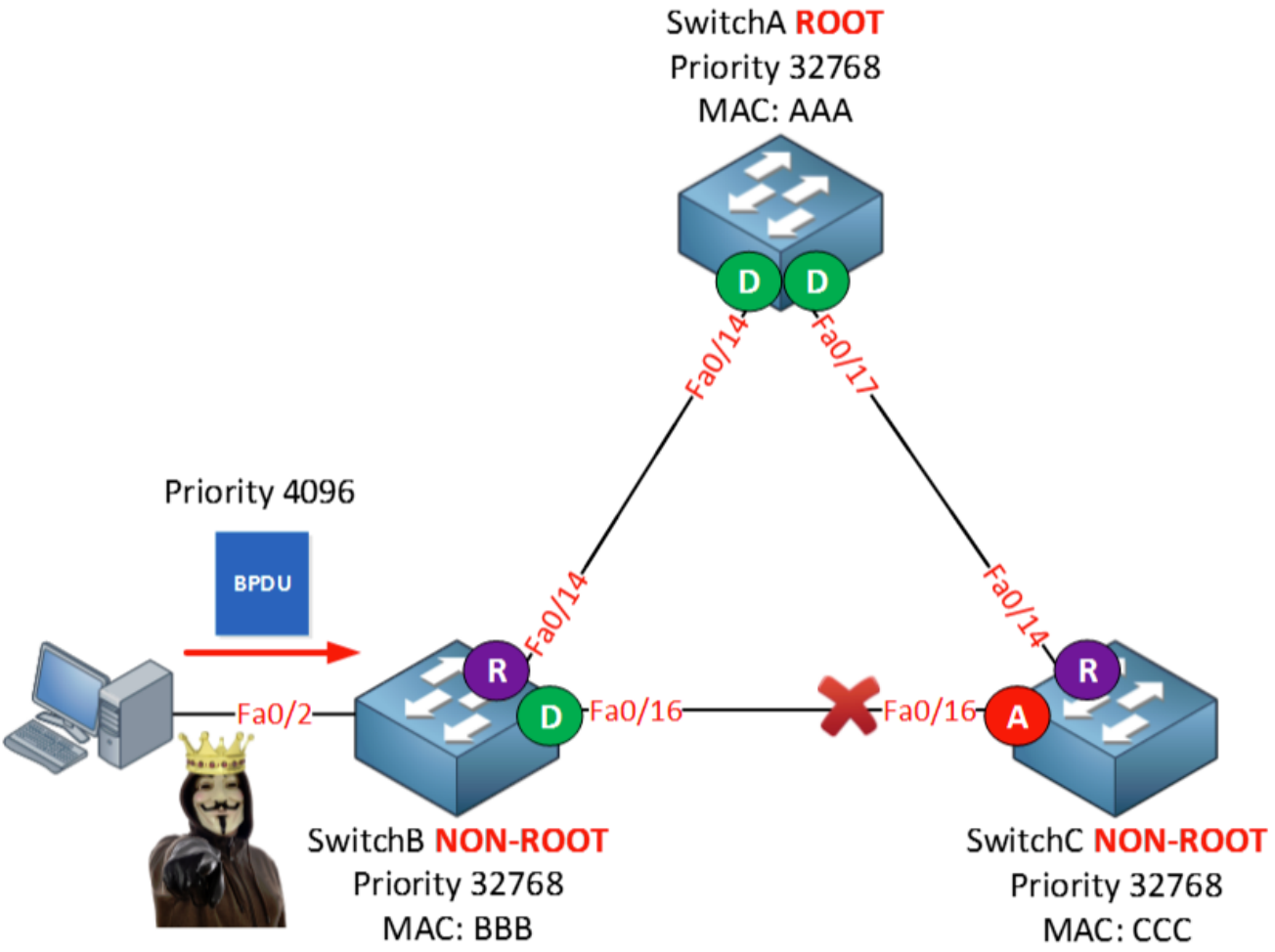
Table of Contents

CCIE Routing & Switching

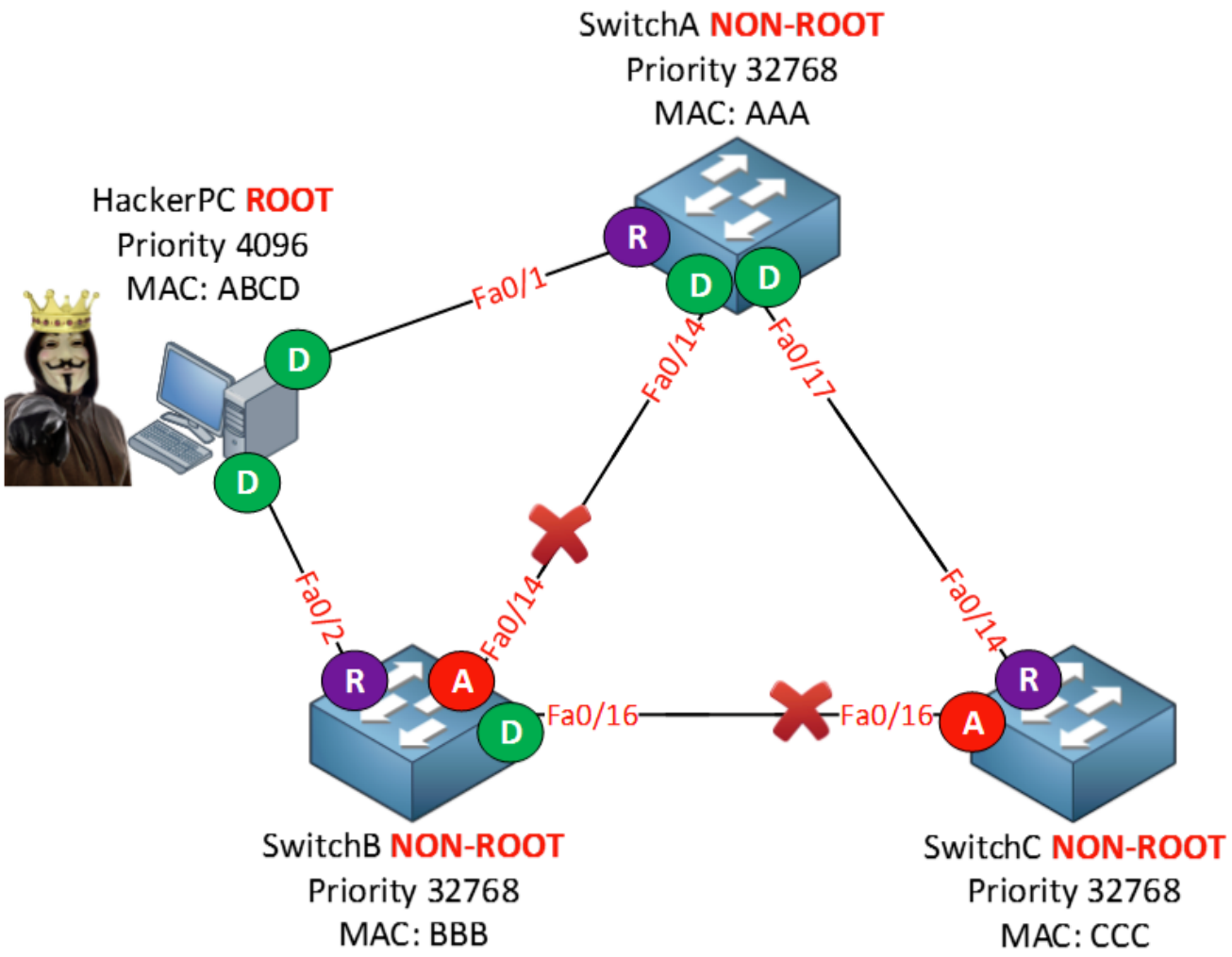
Spanning-Tree BPDUGuard


14 votes

Spanning-tree BPDUguard is one of the features that helps you protect your spanning-tree topology. Let me give you an example:

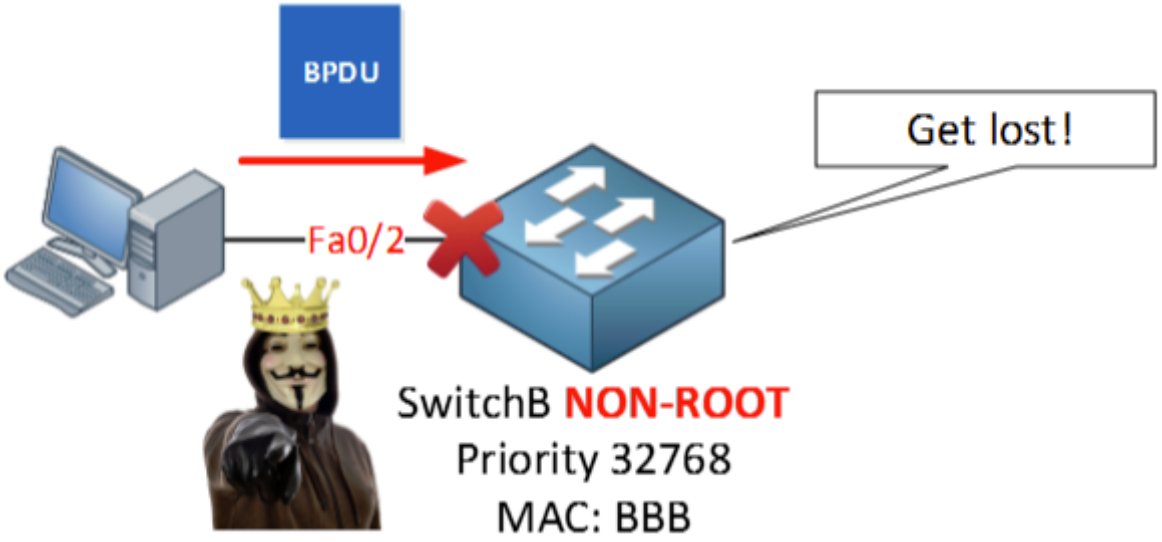


In my topology above we have a perfectly working spanning tree topology. By default spanning tree will send and receive BPDUs on all interfaces. In our example we have a computer on the fa0/2 interface of SwitchB. Someone with ~~curious~~ hostile intentions could start a tool that generates BPDUs with a superior bridge ID. What'll happen is that our switches will believe that the root bridge can now be reached through SwitchB and we'll have a spanning tree re-calculation. Doesn't sound like a good idea right? Here's what could go wrong:



You could even do a man in the middle attack without anyone knowing. Imagine I connect my computer to two switches. If I become the root bridge all traffic from SwitchA or SwitchC towards SwitchB will flow through me. I'll run Wireshark and wait till the magic happens.

We can use BPDUGuard to prevent this from happening as it will block BPDUs:

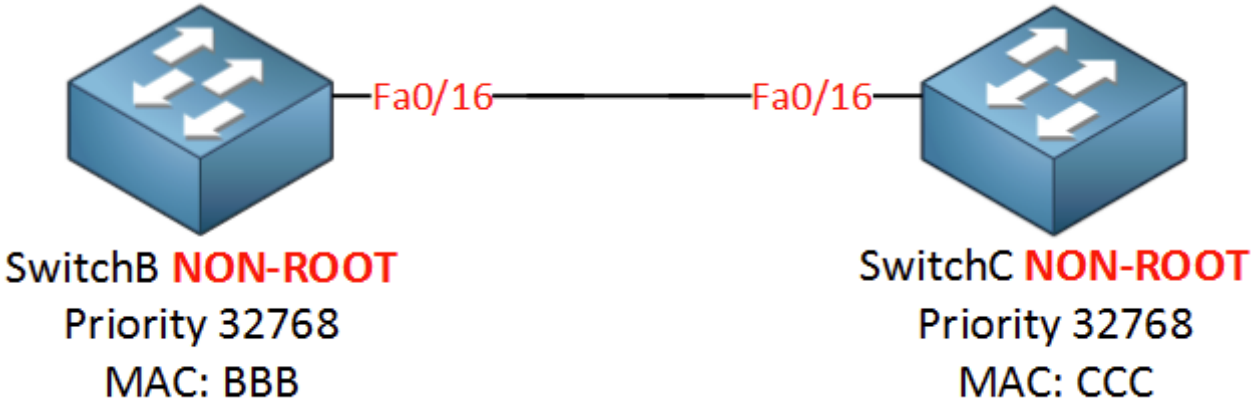


BPDUguard will ensure that when we receive a BPDU on an interface that the interface will go into **err-disable mode**.

Let's take a look how to configure this...

Configuration

I will use the following topology:



To demonstrate BPDUguard I'm going to use two switches. I'll configure the fa0/16 interface of SwitchB so it will go into err-disable mode if it receives a BPDU from SwitchC.

```
SwitchB(config)#interface fa0/16
SwitchB(config-if)#spanning-tree bpduguard enable
```

This is how you enable it on the interface. Keep in mind normally you will never do this between switches; you should configure this on the interfaces in access mode that connect to computers.

```
SwitchB#
%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa0/16 with BPDU Guard
enabled. Disabling port.
%PM-4-ERR_DISABLE: bpduguard error detected on Fa0/16, putting Fa0/16 in err-
disable state
: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/16, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
*Mar  1 00:19:32.089: %LINK-3-UPDOWN: Interface FastEthernet0/16, changed
state to down
```

Uh oh...there goes our interface.

```
SwitchB(config-if)#no spanning-tree bpduguard
SwitchB(config-if)#shutdown
SwitchB(config-if)#no shutdown
```

Get rid of BPDUguard and do a shut/no shut to get the interface back up and running.

```
SwitchB(config)#spanning-tree portfast bpduguard
```

You can also use the spanning-tree portfast bpduguard command. This will globally activate BPDUguard on all interfaces that have portfast enabled.

```
SwitchB(config)#spanning-tree portfast default
```

Portfast can also be enabled globally for all interfaces running in access mode.

```
SwitchB#show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short
```

Here's a useful command so you can verify your configuration. You can see that portfast and BPDUGuard have been enabled globally.

That's all there to it. I hope you enjoyed this lesson!

Rate this Lesson:

« Previous Lesson
MST (Multiple Spanning-Tree)

Next Lesson
Spanning-Tree BPDUFilter »

Home › Forums › Spanning-Tree BPDUGuard

This topic contains 8 replies, has 6 voices, and was last updated by Andrew P 1 month, 1 week ago.

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

- Author
  Posts | Subscribe
- June 22, 2015 at 16:48 #11353 Reply

Georgi T
Participant
awesome explaination Renee .
I really enjoy reading your topics and make me feel more confortable and confident when I learn it
thanks

August 9, 2015 at 04:05 #11354 Reply

Raymond C
Participant
Good stuffs!

November 8, 2015 at 15:48 #19545 Reply

Ahmed A
Participant

Hi Rene,

I am more curious if STP will send BPDUs on Access ports enabled with Portfast or this will be out of the STP topology, Let be more specific with my query

In case i have 2 SWs running RSTP a third SW is introduced which happens to be not supporting STP and is connected to my 2 Sws with portfast enabled

In case BPDUs is being sent on portfast then i assume BPDUGuard will save the day for me on the 2nd SW as it will shut down the port once it receives BPDU on its access port, Is this correct?

November 9, 2015 at 11:26 #19546 Reply

Rene Molenaar
Keymaster
Hi Ahmed,

Enabling portfast doesn't disable STP and the interface will still send BPDUs. Take a look at this post:

https://networklessons.com/spanning-tree/does-portfast-disable-spanning-tree/

In your example, you shouldn't enable portfast on interfaces that connect to other switches. Only use this for "end" devices like computers, laptops, servers, etc. In your case, BPDUguard will ensure that the interface will go down.

Mixing PVST and rapid PVST is no problem btw, they are compatible.

Rene

November 9, 2015 at 14:51 #19554 Reply

Ahmed A
Participant
Thanks Rene, The point here is usually you don't know the end host capability, I saw cases loop can happen from a server with NIC bridging without STP capability.

Just wanted to make sure Portfast + BPDUGuard can address this case

November 9, 2015 at 16:42 #19558 Reply

Rene Molenaar
Keymaster
Hi Ahmed,

In that case it might be wise to enable BPDUguard. If someone connects something that isn't supposed to send BPDUs then it's best to shut the interface with BPDUguard 🙂

Rene

May 13, 2016 at 09:15 #24079 Reply

sims
Participant
Hi,

spanning-tree portfast is enough ? or also spanning-tree portfast bpduguard must be enaled globally

Thanks

May 13, 2016 at 14:24 #24099 Reply

Andrew P
Moderator

Sims,
In almost all cases you want to pair BPDUGuard with Portfast

- Author
  Posts

Viewing 8 posts - 1 through 8 (of 8 total)
Reply To: Spanning-Tree BPDUGuard

b / link b-quote del 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:
Выберите файл Файл не выбран
Add another file

Submit

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!

Read my story

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

Spanning-Tree BPDUGuard written by Rene Molenaar average rating 5/5 - 14 user ratings