



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](#)

Spanning-Tree RootGuard

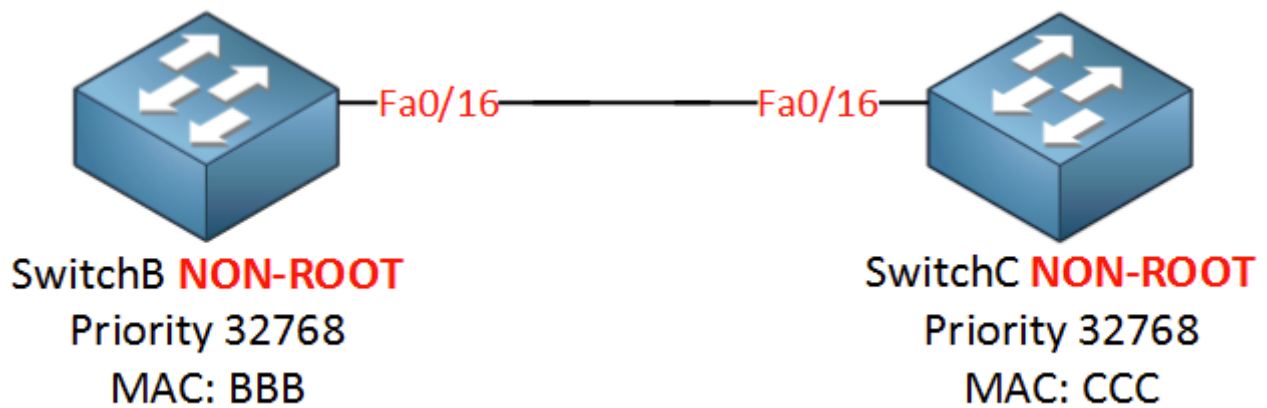


12 votes



RootGuard will make sure you don't accept a certain switch as a root bridge. BPDUs are sent and processed normally but if a switch suddenly sends a BPDU with a superior bridge ID you won't accept it as the root bridge. Normally SwitchB would become the root bridge because it has the best bridge ID, fortunately we have RootGuard on SwitchC so it's not going to happen!

Let me demonstrate this with the following topology:



Let me show you the configuration by using SwitchB and SwitchC, first I will make sure that SwitchC is NOT the root bridge:

```
SwitchB(config)#spanning-tree vlan 1 priority 4096
```

Now we'll enable rootguard on SwitchB:

```
SwitchB(config)#interface fa0/16
SwitchB(config-if)#spanning-tree guard root
%SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root guard enabled on port
FastEthernet0/16.
```

We get a nice notification message that it has been enabled. Let's enable a debug so we can see what is going on:

```
SwitchB#debug spanning-tree events
Spanning Tree event debugging is on
```

Now we'll upset SwitchB by changing the priority to the lowest value possible (0) on SwitchC. Normally it should now become the root bridge:

```
SwitchC(config)#spanning-tree vlan 1 priority 0
```

Let's see what SwitchB thinks about this:

```
SwitchB#
```

```
STP: VLAN0001 heard root      1-000f.34ca.1000 on Fa0/16
supersedes  4097-0019.569d.5700
%SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/16 on
VLAN0001.
```

Here goes...SwitchB will not accept SwitchC as a root bridge. It will block the interface for this VLAN. Here's another useful command to verify this:

```
SwitchB#show spanning-tree inconsistentports
```

Name	Interface	Inconsistency
VLAN0001	FastEthernet0/16	Root Inconsistent

```
Number of inconsistent ports (segments) in the system : 1
```

It's telling us that Fastethernet0/16 is inconsistent. Rootguard is a useful command to enable on your Core or Distribution layer switches so that the underlying switches will never be elected as a root bridge.

Rate this Lesson:




« Previous Lesson
Spanning-Tree BPDUFilter

Next Lesson »
Spanning-Tree LoopGuard and
UDLD



[Home](#) › [Forums](#) › Spanning-Tree RootGuard

This topic contains 14 replies, has 8 voices, and was last updated by  Andrew P 1 month, 1 week ago.

Viewing 14 posts - 1 through 14 (of 14 total)

- Author
Posts | [Subscribe](#)
- May 29, 2015 at 18:43 [#11338 Reply](#)



Srinivasan C

Participant

Hi Rene,

Simple and short explanation makes very easy to understand . One small question..?

Since Root bridge is specific to Switch , Is there any command to enable the Root guard globally ?

If No, We have to enable the "spanning-tree guard root" in all the Designated Ports of Root bridge to make it always root.

Please correct me If I misunderstood the concept here.

Thanks,

Srini

May 30, 2015 at 13:14 [#11339 Reply](#)



Rene Molenaar

Keymaster

Hi Srini,

Root guard is always enabled per interface. Each switch will always elect one interface as its root port (unless the switch is the root bridge). The only thing this command does is ensuring that an interface can never become the root port.

Rene

May 31, 2015 at 19:35 [#11340 Reply](#)



Srinivasan C

Participant

Thanks!

-Srini



August 31, 2015 at 01:30 [#11341 Reply](#)



Thomas K
Participant

Rene,
Hi. Couple questions.

1. I have seen some documents out there that recommend or advise to enable "root guard" on ports connected to end hosts at an access layer switch. Is there any value to still configure root guard if have those end host ports on the access layer switch configured with BPDU-guard & portfast?

2. I see where you advise above to configure rootguard on distribution or core layer switches – if I have a "V" design as indicated below, is there still any value of configuring root guard on the designated port of Switch 1 and the root port of Switch 2? Assume that I have configured SW 1 as the root bridge and SW 2 as the backup root bridge via manipulation of priorities.

Sw 1 Sw 2

/

/

/

switch 3

Many thanks for your time.

August 31, 2015 at 01:31 [#11342 Reply](#)



Thomas K
Participant

Drawing didn't turn out very well essentially I don't have a link between SW1 and SW2 and a communication between those switches is via/through switch 3.



September 6, 2015 at 22:11 [#11343 Reply](#)



Rene Molenaar
Keymaster
Hi Thomas,

1. I would prefer BPDU guard on the access layer switches towards the hosts. You don't want to see any BPDUs from the hosts, if you see them then someone has been messing with bridge mode (bridging two NICs) or they connected a switch, one exception could be a wireless access point. Some of those send BPDUs. If you have BPDU guard enabled, there's no need to use root guard since a BPDU triggers a violation.

We use root guard on interfaces where we DO want to receive BPDUs from but we don't want to accept a root switch on these interfaces.

2. Take a look at this picture:

<https://networklessons.com/wp-content/uploads/2015/03/hierarchical-network-redundant-links.png>

In a network like this, you probably want one of the core switches to be the root bridge and the other one to be the backup. Your core switches should never accept a distribution switch as a root so you could configure root guard on the core interfaces that connect to the distribution switches.

Your distribution switches also should never accept the access layer switches as a root...so on the distribution switch interfaces facing the access layer, enable root guard.

In your example with SW1, SW2 and SW3. You want to make sure that SW1 or SW2 always remains the root. If someone gets access to SW3 and sets the STP priority to 0, it would normally become the root bridge. If you use root guard on SW1 or SW2 then you can prevent this without disturbing STP operations.

Hope this helps!

Rene

February 15, 2016 at 18:29 #22147 Reply



Jie C

Participant

Hi Rene,

I have a question regarding to BPDU guards. If there is a hacker hanging his pc towards en access port lets say vlan 100. And the core is running mst with instace 1 vlan 100 and vlan 200. If the hacker generate a superior bpdu, would it say he can make his pc as root for vlan 100 and 200? But it is connecting to vlan 100 only, if not what would the scenario be?

February 17, 2016 at 16:42 #22186 Reply





Rene Molenaar
Keymaster
Hi Jie,

On the “outside” of the MST region the switches will send PVST “compatible” BPDUs. If the interface is a trunk then you will see a BPDU on each VLAN. If it’s an access port then you will see BPDUs for that VLAN only.

So in this case, the attacker would see BPDUs for VLAN 100.

Catalyst switches with modern IOS images will refuse any 802.1Q tagged frames received on interfaces in access mode. An attacker should be able to send superior BPDUs for VLAN 100 but that’s it.

Rene

March 9, 2016 at 17:59 [#22628 Reply](#)



Hakam A
Participant
Hi

i’ve been uploaded the topology i’m working on while i enable rootguard on the root switch which connected to other non root bridges with two cables per each and try to minimize the priority id on other bridges i lose connectivity to all other non root switches..would you help?

March 10, 2016 at 15:41 [#22638 Reply](#)



Rene Molenaar
Keymaster
Hi Hakam,



Are you getting any error messages? Normally enabling root guard is safe on the root bridge. It will only start blocking the interface when you receive a superior BPDU from a non-root bridge.

Rene

April 30, 2016 at 23:01 [#23711 Reply](#)



Nicholas M
Participant

Will the port that gets the superior BPDU be put in an err-disabled state ?

May 1, 2016 at 00:45 [#23720 Reply](#)



Andrew P
Moderator

Nicholas,

As long as the port continues to receive a superior BPDU, it is placed into "Root-Inconsistent" state which will disable it. Once the superior BPDUs stop being received, the port will automatically recover.

May 10, 2016 at 14:23 [#24004 Reply](#)



Mohammad Hasanuz Z
Participant
Hlw Rene,

Refer to reply [September 6, 2015 at 22:11]

If we do accordingly [enable Root Guard on Core SW, Distribution SW] then all access layer Switch will be disconnected from Core , Distributed and all user will be hampered who are getting service thru the switches. So My Opinion is to enable Root Guard on User facing interface , if any one sending superior BPDU then that user will be hampered not all User , right ??

br//
zaman

May 10, 2016 at 19:39 [#24011 Reply](#)



Andrew P
Moderator



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



VRF Lite Configuration on Cisco IOS



Cisco Portfast Configuration



IPv6 Address Types



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 RootGuard written by Rene Molenaar average rating 4.3/5 - 12 user ratings

