Table of Contents

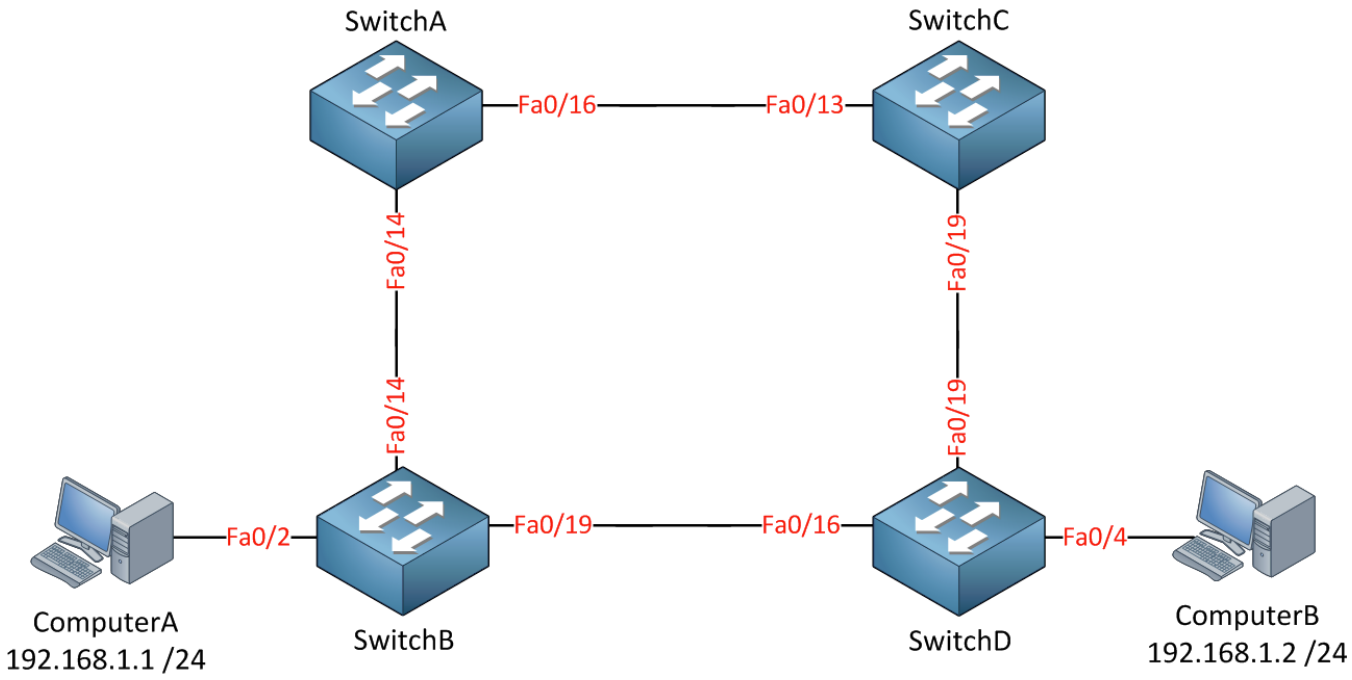
CCIE Routing & Switching

Spanning Tree Topology Change Notification (TCN)


15 votes

How does spanning-tree deal with topology changes? This is a topic that isn't (heavily) tested on the CCNP SWITCH exam but it's very important to understand if you deal with a network with a lot of switches.

Let me show you an example so I can explain a couple of things:



Let's take a look at the picture above. We have two computers because I need something to fill the MAC address tables of these switches. All switches have the default configuration.

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

```
SwitchB(config)#interface fa0/19
SwitchB(config-if)#spanning-tree cost 50
```

I want SwitchC to be the root bridge and the fa0/19 interface of SwitchB should be blocked. I'll show you why in a minute. Let's see what the state is of all these interfaces:

```
SwitchA#show spanning-tree | begin Interface
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
--
Fa0/14              Desg FWD 19        128.16   P2p
Fa0/16              Root FWD 19        128.18   P2p
```

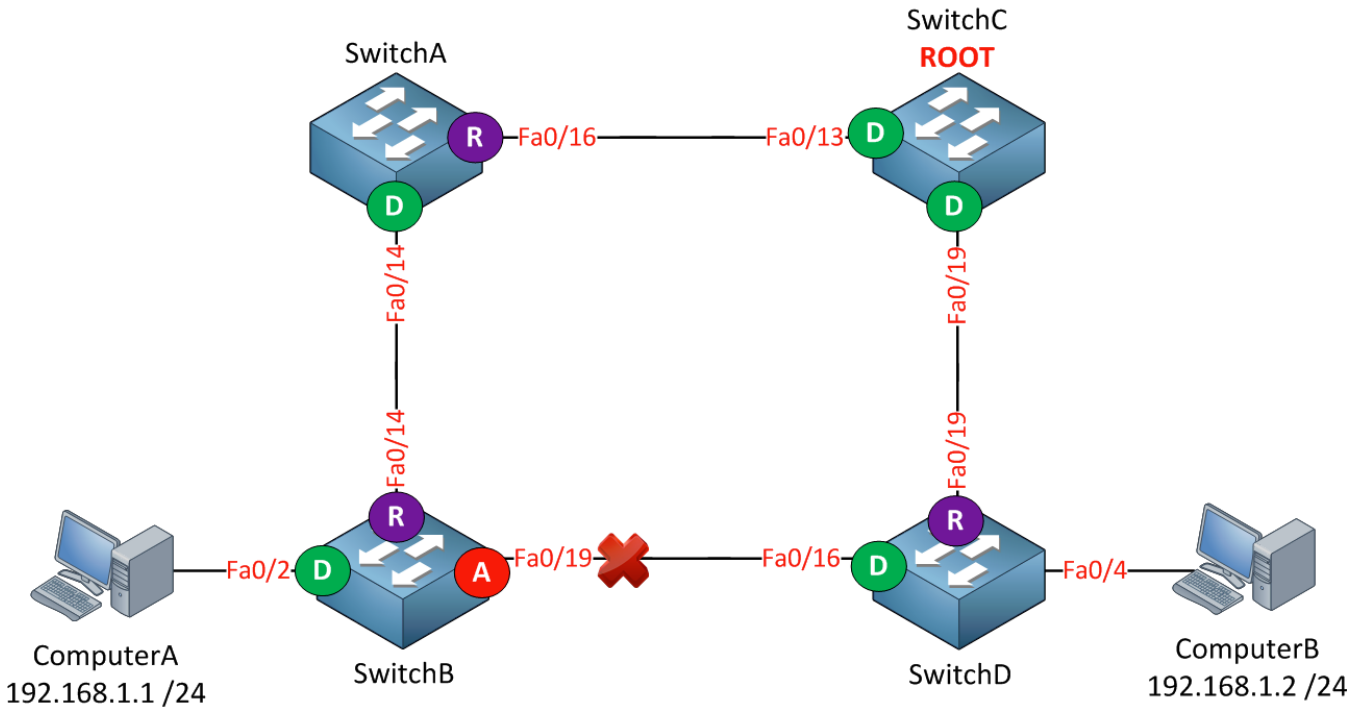
```
SwitchB#show spanning-tree | begin Interface
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
--
Fa0/2               Desg FWD 19        128.4    P2p
```

```
Fa0/14              Root FWD 19        128.16   P2p
Fa0/19              Altn BLK 50        128.21   P2p
```

```
SwitchC#show spanning-tree | begin Interface
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/13           Desg FWD 19        128.13   P2p
Fa0/19           Desg FWD 19        128.19   P2p
```

```
SwitchD#show spanning-tree | begin Interface
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
--
Fa0/4               Desg FWD 19        128.4    P2p
Fa0/16              Desg FWD 19        128.16   P2p
Fa0/19              Root FWD 19        128.19   P2p
```

So here we have all the different interfaces, time to draw a nice picture!



Traffic between ComputerA and ComputerB will flow from SwitchB to SwitchA, SwitchC and then towards SwitchD. Interface fa0/19 on SwitchB has been blocked.

Let's generate some traffic so the switches learn the MAC addresses of the computers:

```
C:Documents and SettingsComputerA>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
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

A simple ping will generate some frames and the switches will learn the MAC addresses.

In my case these are the MAC addresses for the computers:

- ComputerA: 000c.2928.5c6c
- ComputerB: 000c.29e2.03ba

```
SwitchA#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    000c.2928.5c6c    DYNAMIC     Fa0/14
   1    000c.29e2.03ba    DYNAMIC     Fa0/16
```

```
SwitchB#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    000c.2928.5c6c    DYNAMIC     Fa0/2
   1    000c.29e2.03ba    DYNAMIC     Fa0/14
```

```
SwitchC#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    000c.2928.5c6c    DYNAMIC     Fa0/13
   1    000c.29e2.03ba    DYNAMIC     Fa0/19
```

```
SwitchD#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    000c.2928.5c6c    DYNAMIC     Fa0/19
   1    000c.29e2.03ba    DYNAMIC     Fa0/4
```

We can confirm the traffic path by looking at the MAC address table. I like to use the **show mac address-table dynamic** command so we don't have to browse through a list of static MAC addresses.

Do you have any idea how long a switch will store a MAC address?

```
SwitchA#show mac address-table aging-time
Global Aging Time:  300
```

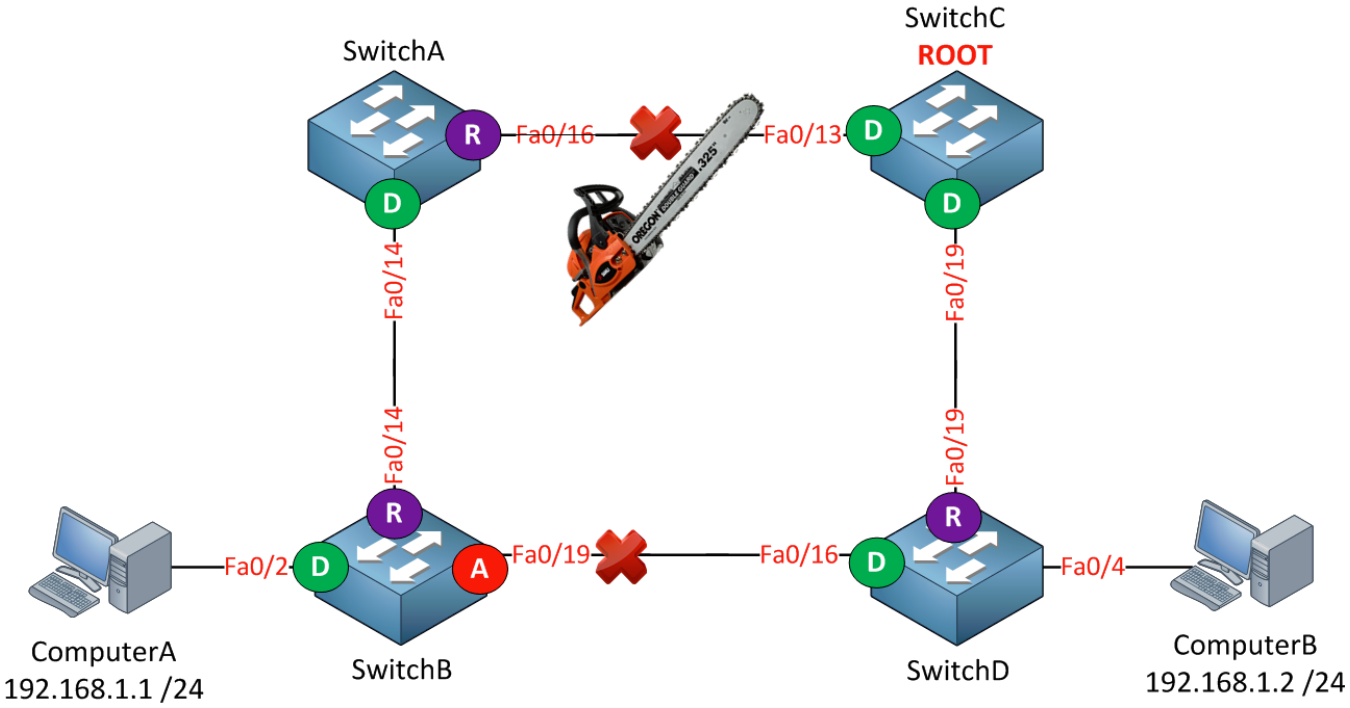
If we look at one of the switches we can check the default aging time of the MAC address table. As you can see this is **300 seconds** (5 minutes by default). If a host has been silent for 5 minutes its MAC address will be removed from the table.

Why do we care about aging time? I'll show you why!

```
C:Documents and SettingsComputerA>ping 192.168.1.2 -t
```

First I'm going to get some traffic going from ComputerA to ComputerB. By using ping –t it will run forever.

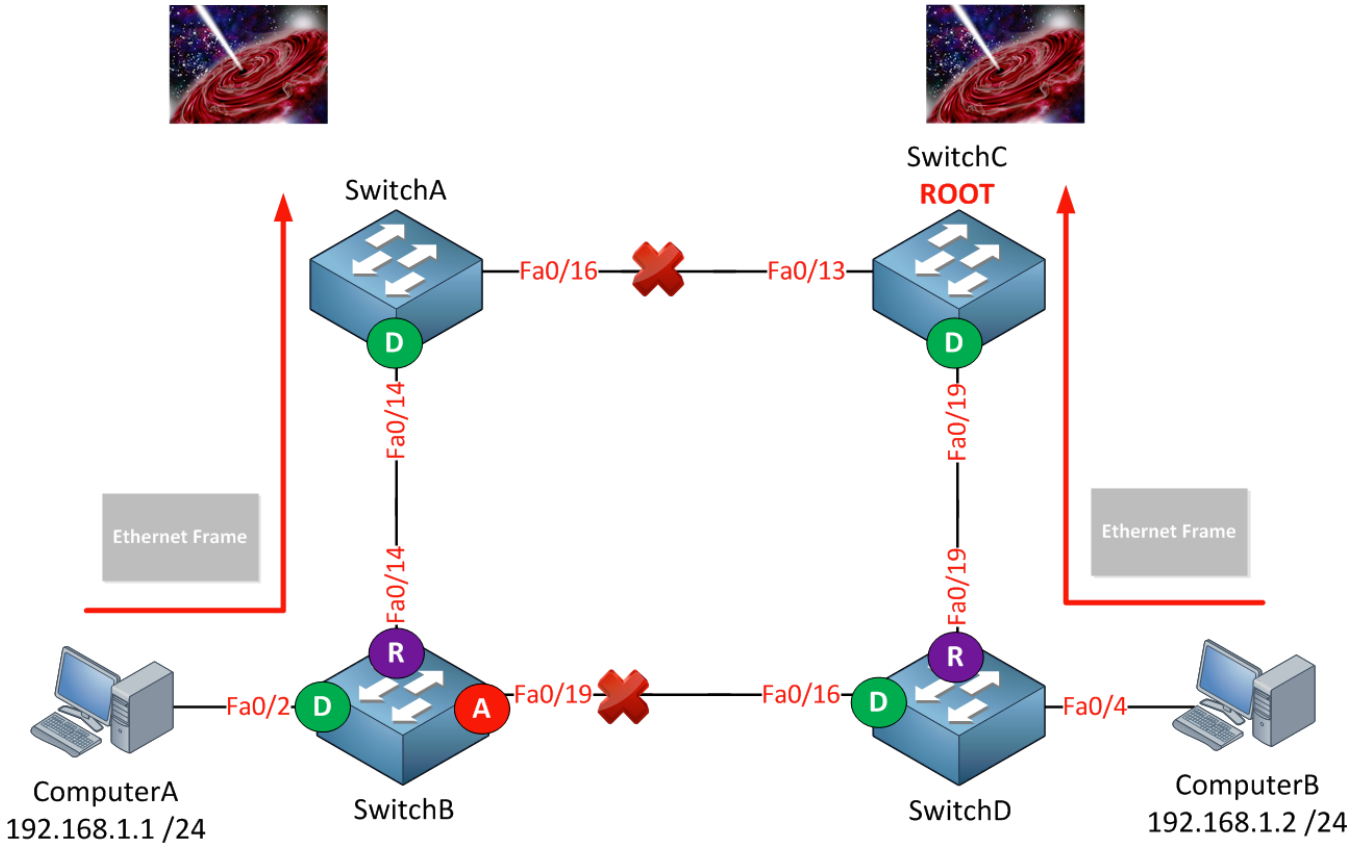
The next step will be to unplug one of the cables:



Assume the link between SwitchA and SwitchC fails. ComputerA and ComputerB will be unable to communicate with each other until the fa0/19 interface of SwitchB goes into forwarding.

It will take a maximum of 50 seconds for SwitchB to move the fa0/19 interface from blocking to listening, learning and finally the forwarding state.

Meanwhile SwitchB still has the MAC address of ComputerB in its MAC address table and will keep forwarding it to SwitchA where it will be dropped. It will be impossible for our computers to communicate with each other for 300 seconds until the MAC address tables age out.



"Sending Ethernet frames to a place where no frame has gone before doesn't sound like a good idea if you want to keep your users happy..."

The idea of MAC address tables that age out after 300 seconds works perfectly fine in a stable network but not when the topology changes. Of course there's a solution to every problem and that's why spanning-tree has a topology change mechanism.

When a switch detects a change in the network (interface going down or into forwarding state) it will advertise this event to the whole switched network.

When the switches receive this message they will reduce the aging time of the MAC address table from 300 seconds to 15 seconds (this is the forward delay timer). This message is called the TCN (Topology Change Notification).

To take a closer look at the TCN we'll have to do some debugging...

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

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

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

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

I'm going to enable debug spanning-tree events on all switches so you can see this process in action.

Now we will shut the Interface fa0/16 on SwitchA to simulate a link failure:

```
SwitchA(config)#interface fa0/16
SwitchA(config-if)#shutdown
```

Here's what you'll see:

```
SwitchA#STP: VLAN0001 sent Topology Change Notice on Fa0/14
```

You will see quite some debug information but somewhere along the lines you'll see that SwitchA is generating a topology change notification and sends it on its fa0/14 interface to SwitchB. Here's what you see on SwitchB:

```
SwitchB#STP: VLAN0001 Topology Change rcvd on Fa0/14
```

SwitchB will throw quite some debug stuff in your face but this is what I was looking for. You can see that it received the topology change notification from SwitchA. Upon arrival of this topology change notification SwitchB will age out its MAC address table in 15 seconds.

What will SwitchB do with this information? Look below:

```
SwitchB#STP: VLAN0001 new root port Fa0/19, cost 69
SwitchB#STP: VLAN0001 Fa0/19 -> listening
SwitchB#STP: VLAN0001 Topology Change rcvd on Fa0/14
SwitchB#STP: VLAN0001 sent Topology Change Notice on Fa0/19
SwitchB#STP: VLAN0001 Fa0/19 -> learning
SwitchB#STP: VLAN0001 sent Topology Change Notice on Fa0/19
```

```
SwitchB#STP: VLAN0001 Fa0/19 -> forwarding
```

SwitchB decides that fa0/19 is now the new root port and you can see the transition from listening to learning and forwarding mode. It's also sending a topology change notification towards SwitchD.

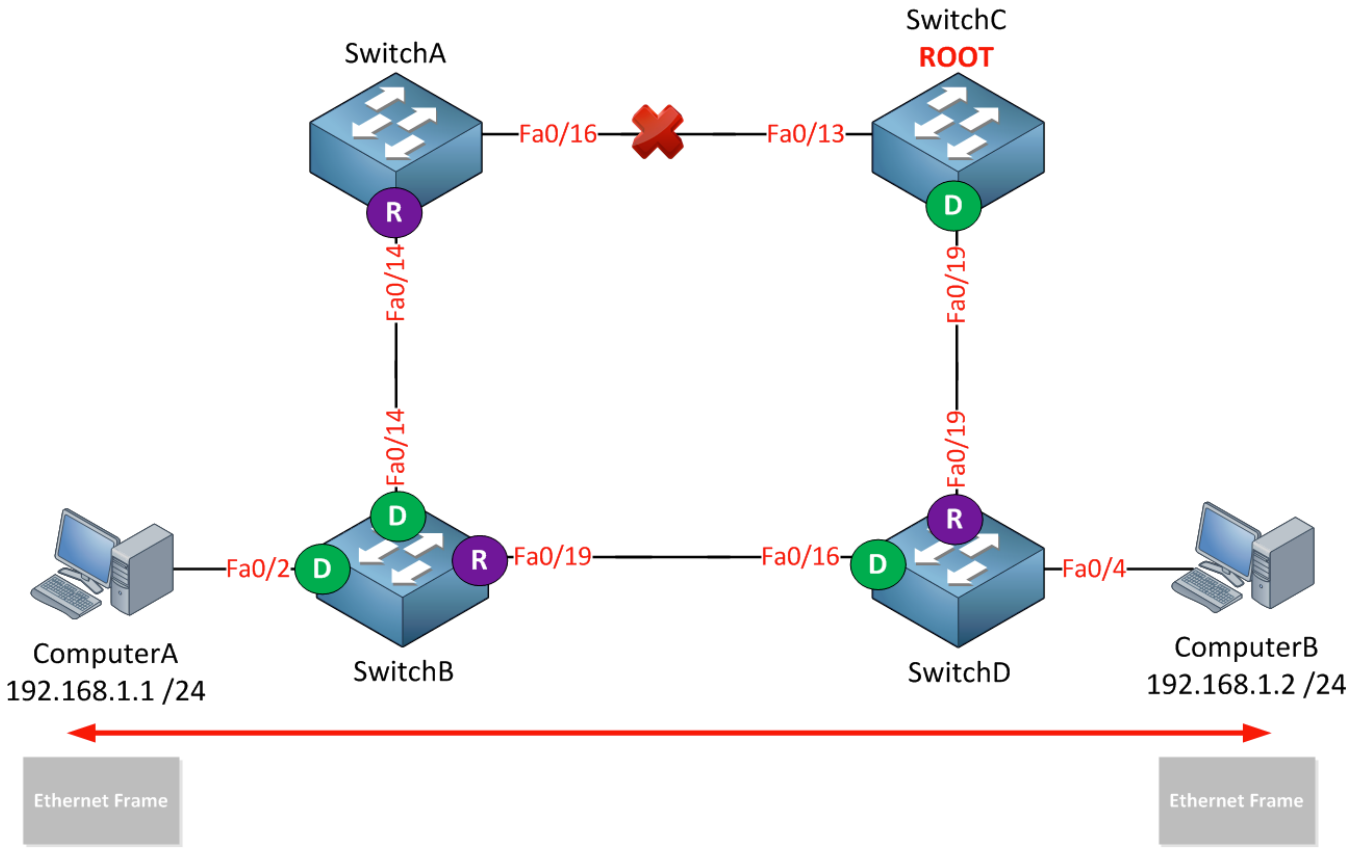
```
SwitchC#STP: VLAN0001 Topology Change rcvd on Fa0/19
```

SwitchC receives a topology change notification on its fa0/19 interface and will reduce its age out timer of the MAC address table to 15 seconds.

```
SwitchD#STP: VLAN0001 Topology Change rcvd on Fa0/16
SwitchD#STP: VLAN0001 sent Topology Change Notice on Fa0/19
```

Here we see that SwitchD receives the topology change notification from SwitchB and as a result it will reduce its age out timer of the MAC address table to 15 seconds. It's also sending a topology change notification to SwitchC.

All switches received the topology change notification and set their age out timer to 15 seconds. SwitchB doesn't receive any Ethernet Frames with the MAC address of ComputerB as the source on its fa0/14 interface and will remove this entry from the MAC address table.

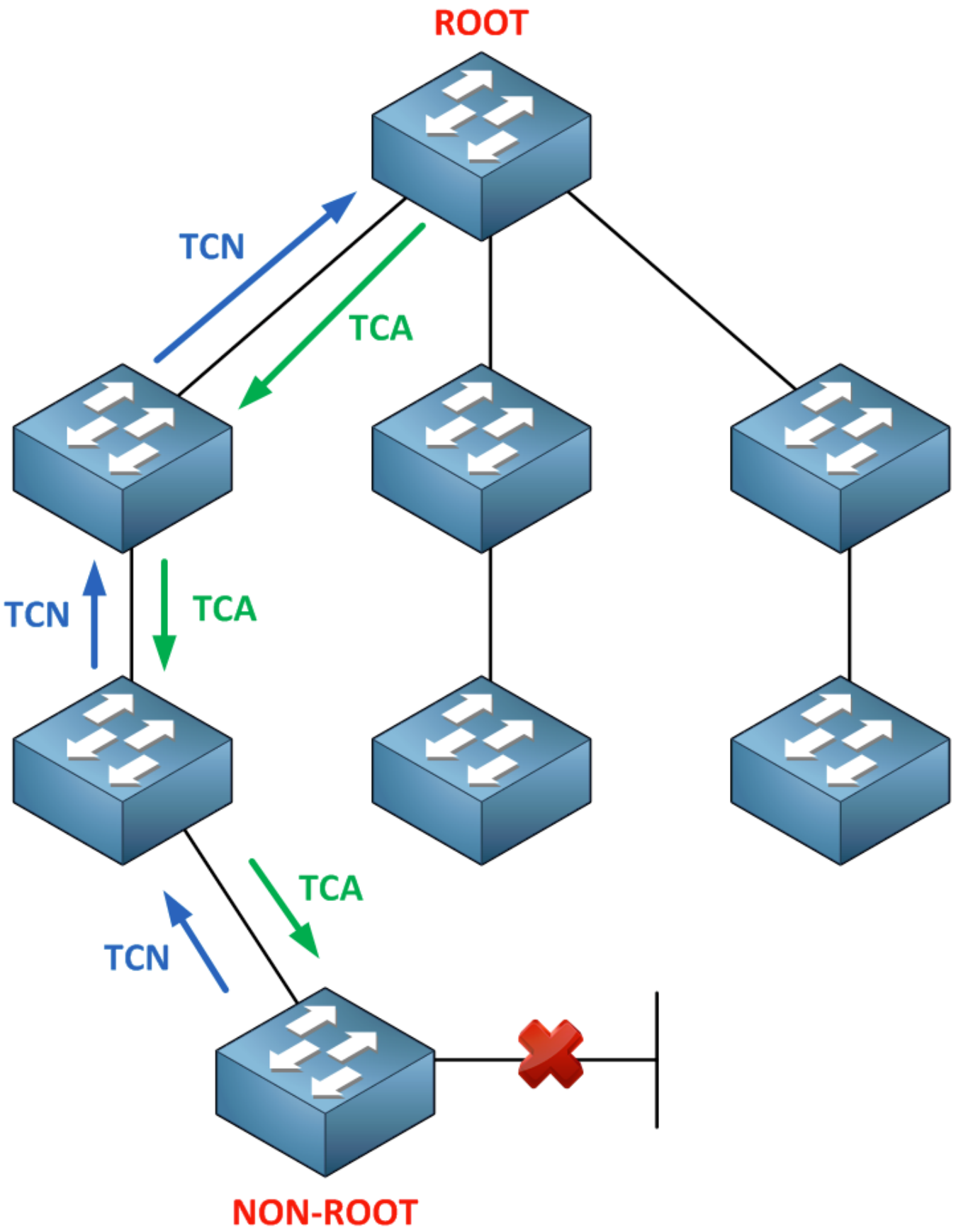


Meanwhile the fa0/19 interface on SwitchB changed from blocking to listening, learning and forwarding state (50 seconds total). SwitchB will now learn the MAC address of ComputerB on its fa0/19 interface and life is good!

Of course the same thing will happen for the MAC address of ComputerA on SwitchD.

Are you following me so far? To keep a long story short...we need the topology change notification to reduce the MAC address table aging timer from 300 seconds to 15 seconds to prevent blackholing traffic in a situation like I just explained to you.

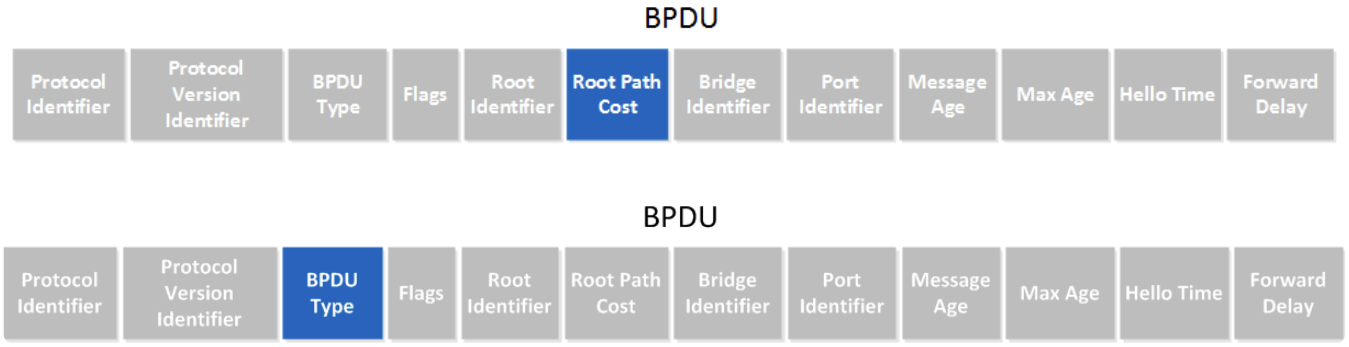
So which switches will send and forward the topology change notifications? In our previous debug you saw a couple of messages but where do we send them and why? Is it flooded to all switches? Let's check it out!



In a normal situation a non-root switch will receive BPDUs on its root port but will never send any BPDUs to the root bridge. When a non-root switch detects a topology change it will generate a topology change notification and send it on its root port towards the root bridge.

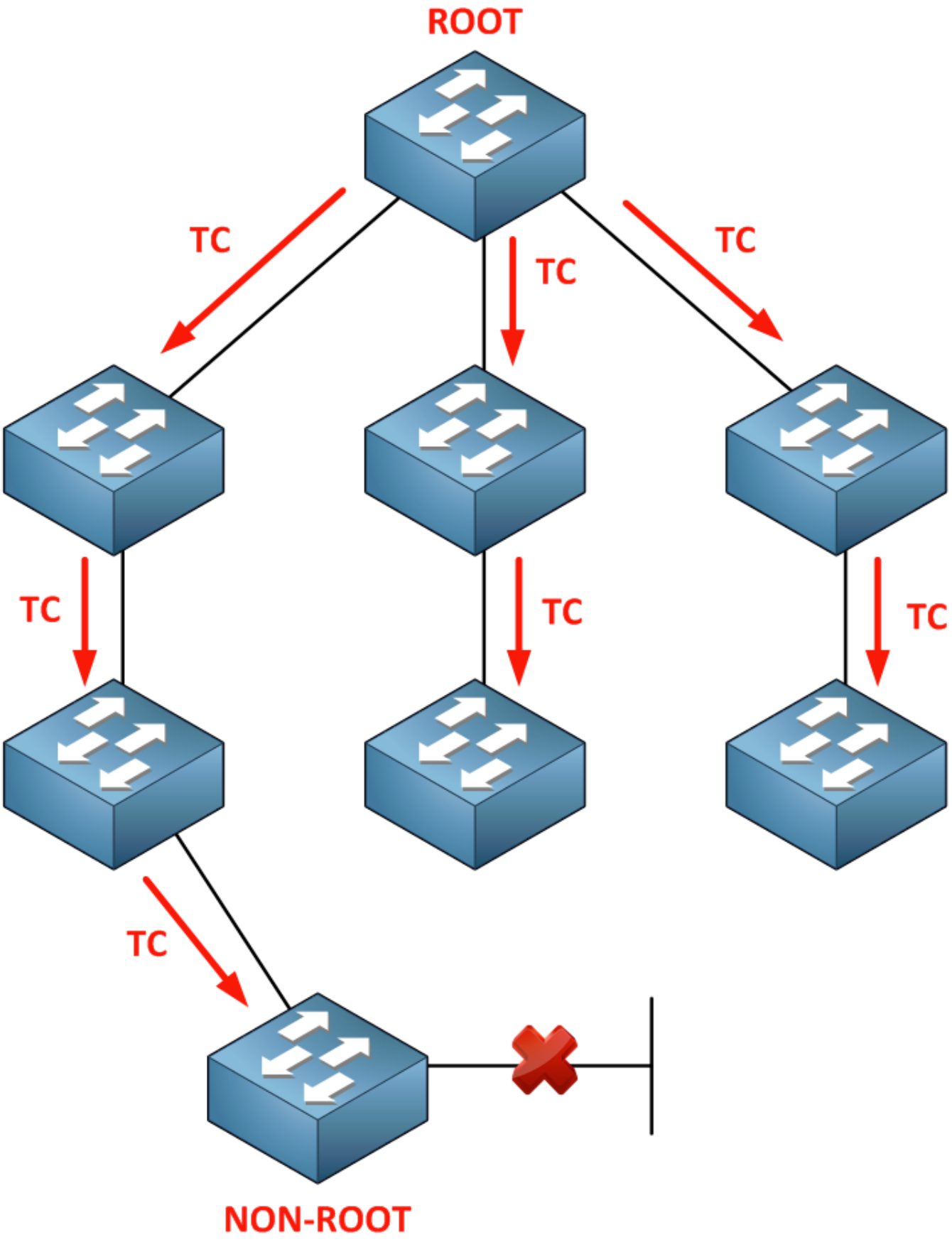
When a switch receives the topology change notification it will send a (TCA) topology change acknowledgement on its designated port towards the downstream switch. It will create a topology change notification itself and send it on its root port as well...we will work our way up the tree until we reach the root bridge.

What kind of message is used for the TCN? Take a look at this BPDU:



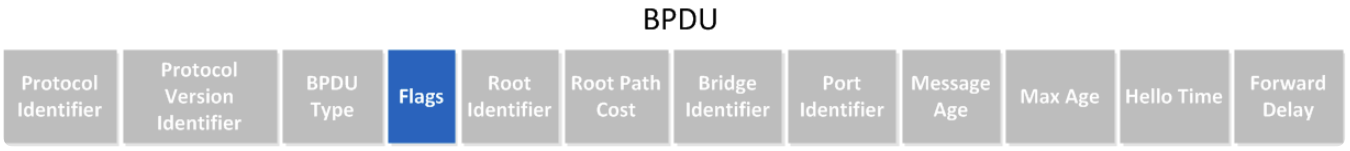
You can see it has a field called BPDU type. This value will change to indicate it's a topology change notification.

Once the topology change notification reaches the root bridge it will set the TC (topology change) bit in the BPDUs it will send.

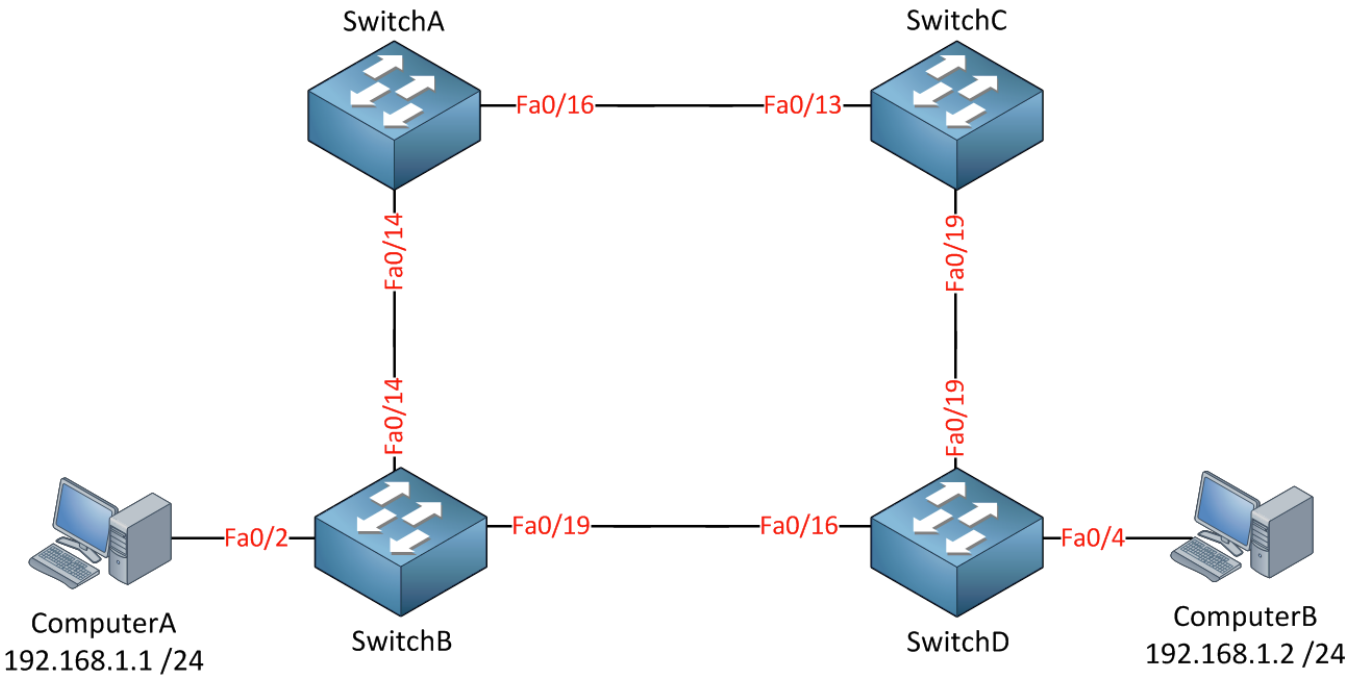


These BPDUs will be forwarded to all the other switches in our network so they can reduce their aging time of the MAC address table. Switches will receives these messages on both forwarding and blocked ports.

The root bridge will send BPDUs and it will set the flag field to represent the topology change.



That's all there is to it. This is how spanning-tree deals with topology changes in our network. There is one more thing I want to you show you about this mechanism. Take a look at the picture below:



As you can see ComputerA is connected to SwitchB on its fa0/2 interface. Let's see what happens when this interface goes down.

```
SwitchB#show spanning-tree interface fa0/2

Vlan                 Role Sts Cost      Prio.Nbr Type
-------------------- ---- --- --------- -------- --------------------------------
--
VLAN0001             Desg FWD 19        128.4    P2p
```

We can see that the fa0/2 interface on SwitchB is designated and forwarding. Let's enable a debug and shut this interface:

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

```
SwitchB(config)#interface f0/2
SwitchB(config-if)#shutdown
```

This is what happens on SwitchB:

```
SwitchB STP: VLAN0001 sent Topology Change Notice on Fa0/14
```

Right after shutting down the fa0/2 SwitchB generates a topology change notification and sends it away on its root port.

Let's bring it up again:

```
SwitchB(config)#interface f0/2
SwitchB(config-if)#no shutdown
```

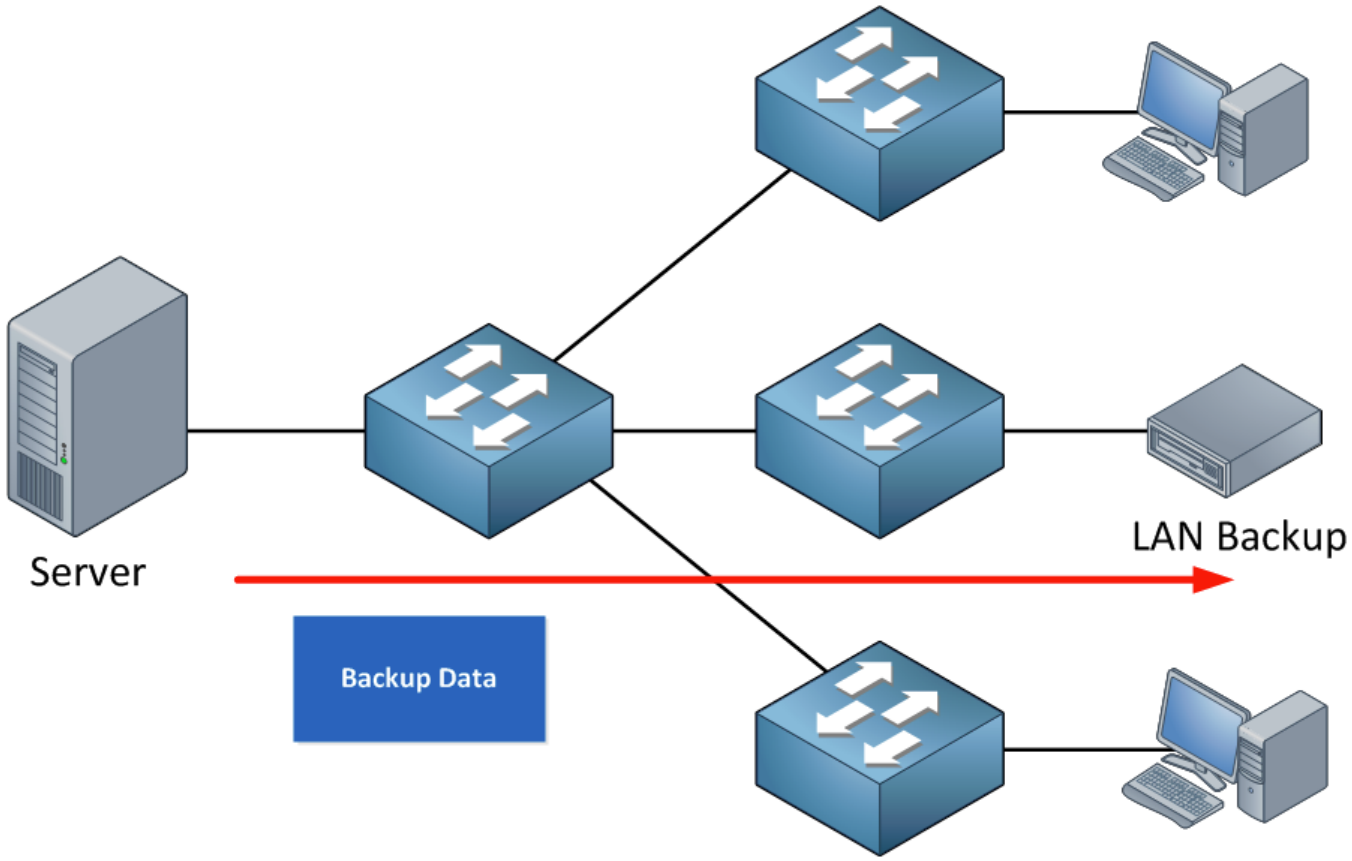
This is what you'll see:

```
SwitchB#  STP: VLAN0001 Fa0/2 -> listening
SwitchB# %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
SwitchB# %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
SwitchB# changed state to up
SwitchB# STP: VLAN0001 Fa0/2 -> learning
SwitchB# STP: VLAN0001 sent Topology Change Notice on Fa0/14
SwitchB# STP: VLAN0001 Fa0/2 -> forwarding
```

Once we bring the interface up you can see it goes through the listening and learning state and ends in the forwarding state. The switch generates another topology change notification and sends it on the root port.

What kind of issues could this cause? Imagine we have a network with a LOT of hosts. Each time an interface goes up or down a topology change notification will be generated and ALL switches will set their aging time to 15 seconds. A host will trigger a topology change and if you have a lot of hosts it’s possible that you end up with a network that is in a constant state of “topology changes”.

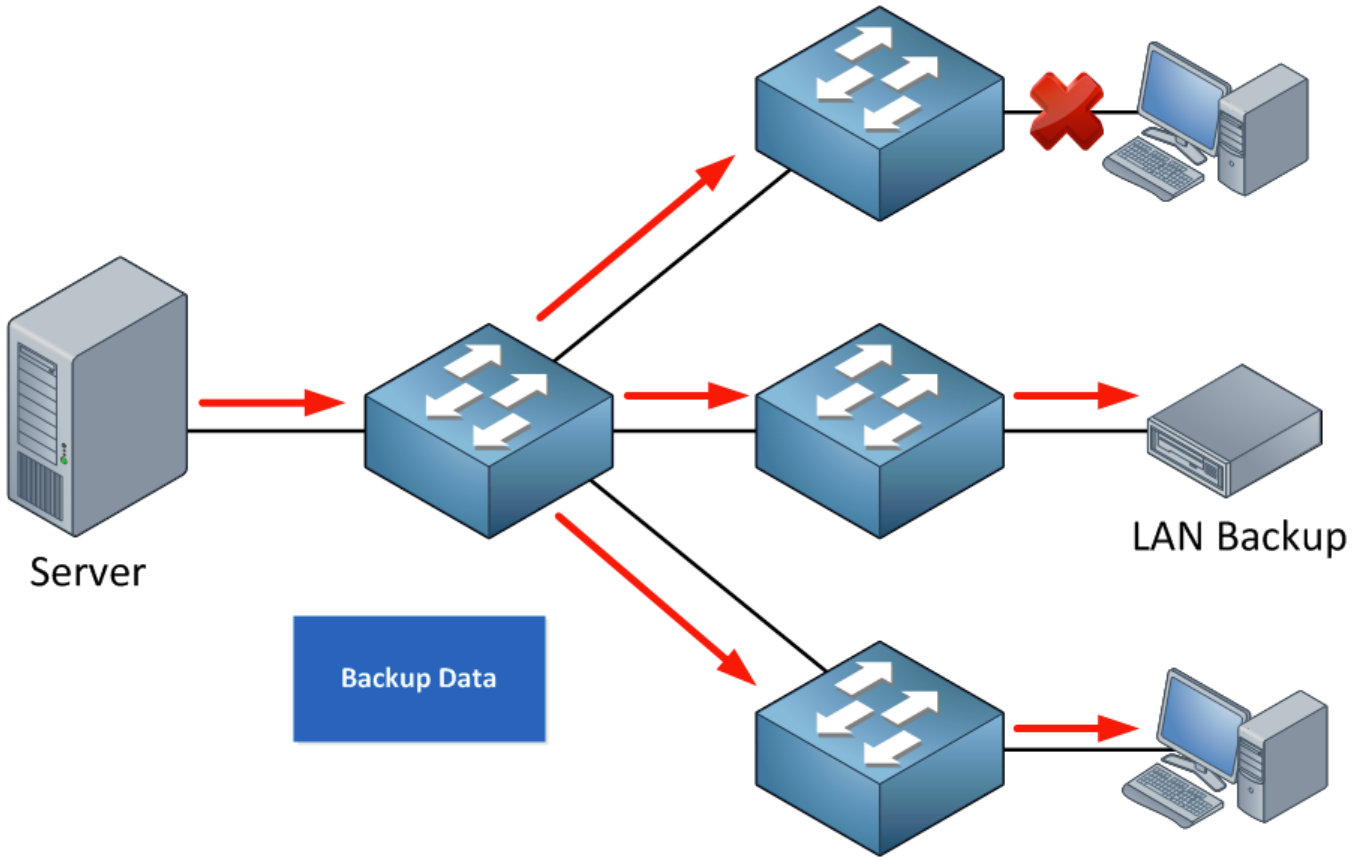
Here’s a situation that could occur:



In the picture above I have a server sending a backup to a LAN backup device. This means we'll probably have a lot of unicast traffic from the server to the LAN backup device.

Whenever an interface goes down it will generate a topology change notification and as a result all switches will reduce their aging time of the MAC address table to 15 seconds. All the MAC addresses of the devices will be flushed from the MAC address table.

The switches will quickly re-learn the MAC address of the server since its actively sending traffic to the LAN Backup device. If this LAN Backup device is just silently receiving traffic and not sending any traffic itself then there's no way for the switches to re-learn its MAC address.



What happens to unknown MAC unicast traffic? That's right...it's flooded on all interfaces except the one where it originated from. As a result this network will be burdened with traffic until our LAN Backup device sends an Ethernet Frame and the switches re-learn its MAC address.

How can we deal with this drama scenario?

Portfast to the rescue! Portfast is a Cisco proprietary solution to deal with topology changes. It does two things for us:

- Interfaces with portfast enabled that come up will go to forwarding mode immediately. It will skip the listening and learning state.
- A switch will never generate a topology change notification for an interface that has portfast enabled.

It's a good idea to enable portfast on interfaces that are connected to hosts because these interfaces are likely to go up and down all the time. Don't enable portfast on an interface to another hub or switch.

Rate this Lesson:

« Previous Lesson
Spanning-Tree Port States

Next Lesson
Spanning-Tree Portfast »

Home › Forums › Spanning Tree Topology Change Notification (TCN)

This topic contains 23 replies, has 14 voices, and was last updated by Andrew P 1 month, 2 weeks ago.

Viewing 15 posts - 1 through 15 (of 23 total)
1 2 →

- Author
  Posts | Subscribe
- January 19, 2015 at 16:12 #11623 Reply

Yevgeniy O
Participant
you're strong man 😉

March 31, 2015 at 12:57 #11624 Reply

Alberto D
Member
There is something that i not understand . I worked with network with many hosts , but I didn't set these in portfast . However there wasn't problem like you mentioned (burned traffic) , why ?

March 31, 2015 at 19:31 #11625 Reply

Rene Molenaar
Keymaster
Hi Alberto,

It's a good practice to disable TCN generation for interfaces that are connected to hosts. An interface that connects to a host/server doesn't change the STP topology so there's no reason to generate TCNs when these interfaces go down. It's possible that you never encountered the downside of not enabling portfast but an example like the problem with the backup server is possible.

Rene

July 3, 2015 at 22:59 #11626 Reply

Atif S
Participant
Little confused towards the end, if portfast is enabled on host end and when host interface goes down how does the mac address get cleared on the switches since the tcn is not sent on portfast ports? after the default 5min age time?

July 5, 2015 at 18:45 #11627 Reply

Rene Molenaar
Keymaster
Hi Atif,

TCNs are only for spanning-tree. When an interface goes down on the switch, it will clear the MAC addresses associated with it.

Rene

September 24, 2015 at 16:14 #11628 Reply

Mauro P
Participant
Hello Rene,

I think now is possible to configure (spanning-tree portfast trunk) for ports in trunk mode. I found that amazing. 🙂

Regards Mauro.

September 24, 2015 at 16:19 #11629 Reply

Rene Molenaar
Keymaster
Hi Mauro,

Yes that's right, it is possible. This can be useful in certain scenarios...for example standalone access points that require a trunk because they use a different VLAN for each SSID.

Rene

November 16, 2015 at 18:57 #19736 Reply

Gbenga R
Participant
thank you for the lesson. it definitely cleared a lot of doubts.

January 4, 2016 at 12:27 #20713 Reply

Chandima E
Participant
Hi Rene

It is a great lesson to understand the Topology change on the STP. I have a question which is related to the switches which receives only BPDU with TCN flag set from the Root bridge

Assume that Switch network has few more switches and TCN notification generated by switch (switch A on the diagram) has not been pass through on these switches . I need to know what would be the mac address aging time for the other switches which receives BPDU's with TCN flag set. My understanding is if a switch in the switch network received the TCN from the Root bridge the switch set the mac address aging time to max-age in the STP.

My other question is, due to some reason when switch does not receive the BPDU, will this switch wait for Max age time (20s) by default to flush the Mac-address table? Then how the STP reconvergence will affect the switch network

Regards

Chandi

January 8, 2016 at 03:25 #20789 Reply

Davis W
Participant
Hi Rene,

By default the Aging time 5 minutes will clear all the Mac address in the table and relearn it or only clear those host MAC address that have no activity for 5 minutes?

Davis

January 8, 2016 at 12:46 #20793 Reply

Rene Molenaar
Keymaster
Hi Davis,

The aging time applies only to specific MAC addresses. Wiping the entire MAC address table every 5 minutes would be a bad idea 🙂

Rene

January 8, 2016 at 14:57 #20796 Reply

Davis W
Participant
Ok. Thanks Rene.

Davis

March 1, 2016 at 07:08 #22486 Reply

shayan a
Participant

Hello Rene,

I am getting confused with this concepts in STP, The more i read the more i am getting confused Please help me upnderstand this concepts, I 've wriiten my understanding and questions.

In a Steady state Network assuming the packet between computer A and Computer B takes (Switch B –> Switch A –> Switch C –> Switch D)

Question related to interface states and convergence time
==========
Switch C (Root Bridge) generates configuration BPDU's and sends it to Switch A and Switch D and in turn they relay it to switch B
When we have an indirect link failure (shutting down the interface between Switch A and Switch C i.e fa0/16)
Switch A will start advertising itself as Root switch to switch B (downstream)
Since the BPDU received at switch B is inferior to the BPDU which it had received earlier, it will start the max-age timer ignoring BPDU's till 20 secs
Once the max-age is expired the interface fa0/19 of switch B will move into Listening state, eventually move out to learning and forwarding
Totally it takes 50 sec for the interface (fa0/19) to move from blocking to Forwarding state
what exactly happens in the listening state ? it will start electing the root switch, root port, dp etc ? is my other understanding are correct ?

Question related to Topology Change
==========
When ever we have a topology change the switch with interface going up/down, will generate a BPDU with TCN flag set and sends it towards the root switch
This is the only time where a non-root switch will generate a BPDU towards the root switch
The switches which receive the BPDU will acknowledge back to the sender switch which generated the TCN and also relay the BPDU towards the root switch
once it reaches the root switch, it will propagate the changes to the entire switch network in that segment
upon receiving on this BPDU every switch in that segment will reduce mag-aging timer to 15 secs
so my question is TCN is more of to do with aging out the mac-table and it has no significance in the interface state changes ?

I've written my understaning and questions. Pleae help me with this questions.

Regards!
Shayan

March 3, 2016 at 07:11 #22517 Reply

shayan a
Participant
Hello Rene,

can you please shed some light on this ? The more I explore the more i am getting confused.

Regards!
Shayan

March 3, 2016 at 14:49 #22528 Reply

Rene Molenaar
Keymaster
Hi Shayan,

If you want to see exactly what is going on in a topology like this I highly recommend to configure 4 switches and to enable “debug spanning-tree events” on all switches. It will show you exactly why and how the interfaces are moving through the different states. It’s much easier to see it then just to read and visualize how it works.

In the listening state we only process BPDUs. This time is used to learn what the STP topology looks like, it’s when we elect ports etc yes.

The main reason for the TCN is to reduce the MAC address table aging timer from 300 to 15 seconds. If we don’t do this then it’s possible that traffic gets blackholed for up to 300 seconds.

Rene

- Author
  Posts

Viewing 15 posts - 1 through 15 (of 23 total)
1 2 →
Reply To: Spanning Tree Topology Change Notification (TCN)

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)

Spanning Tree Topology Change Notification (TCN) written by Rene Molenaar average rating 4.7/5 - 15 user ratings