Networklessons.com

Search...

Table of Contents

CCIE Routing & Switching

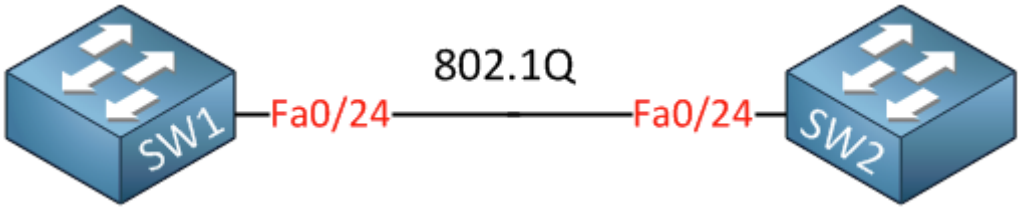
802.1Q Native VLAN on Cisco IOS Switch

14 votes

The IEEE 802.1Q trunking protocol describes something called the “native VLAN”. All traffic sent and received on an interface that is configured for 802.1Q won’t have a tag on its Ethernet frame. When you look at it in Wireshark, it will look the same just like any normal Ethernet frame.

When your Cisco switches receives an Ethernet frame without a tag on a 802.1Q enabled interface, it will assume that it belongs to the native VLAN. For this reason you need to make sure that the native VLAN is the same on both sides.

By default the native VLAN will be VLAN 1 but we can change this if we want. Let's look at an example, I will use two switches for this:



I will configure a 802.1Q trunk between those two switches so we can look at the native VLAN:

```
SW1(config)#interface Fastethernet 0/24
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
```

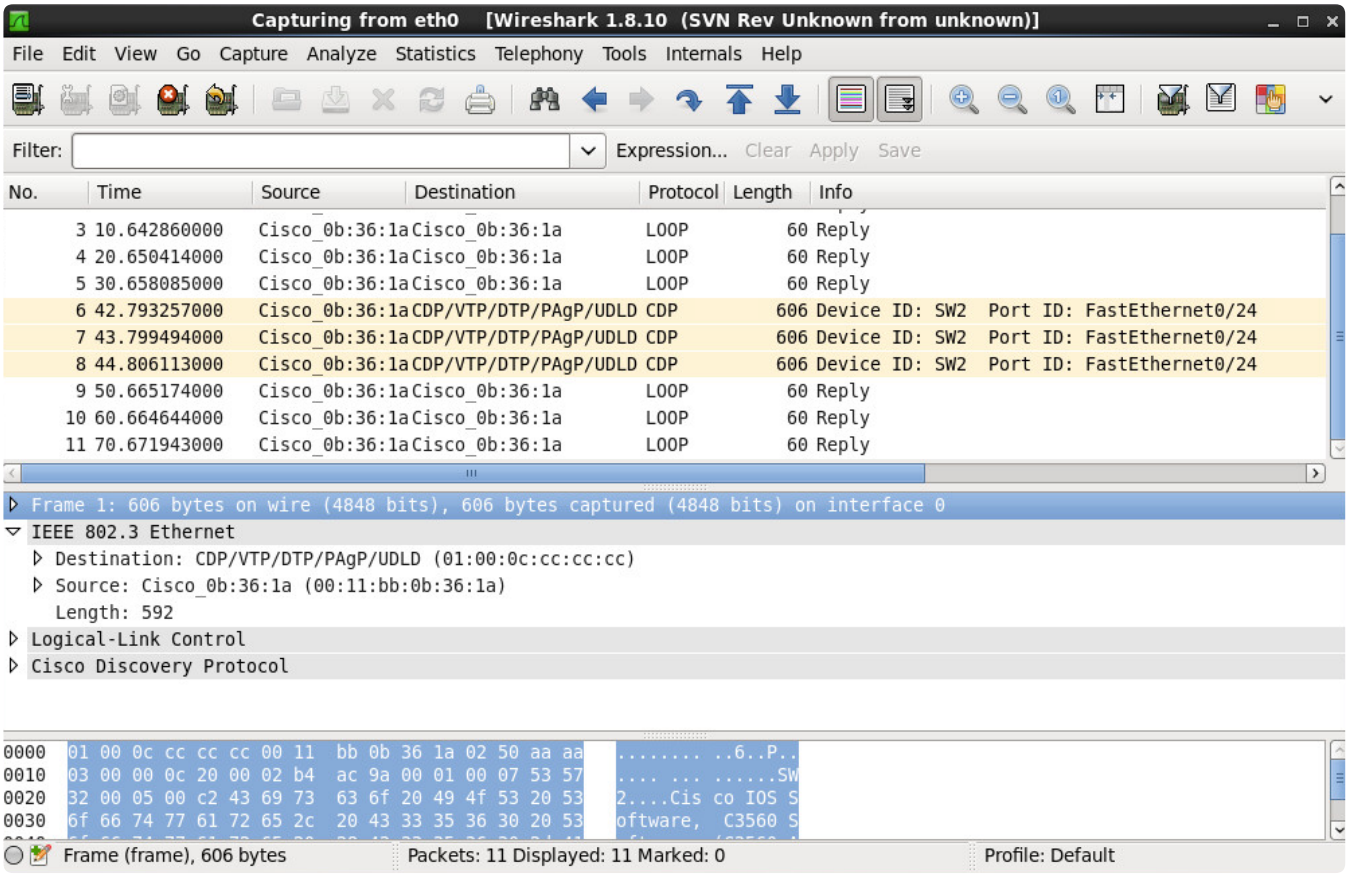
```
SW2(config)#interface Fastethernet 0/24
SW2(config-if)#switchport trunk encapsulation dot1q
SW2(config-if)#switchport mode trunk
```

We can verify our trunk configuration and see the native VLAN like this:

```
SW1#show interface fastEthernet 0/24 trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/24      on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/24      1-4094

Port        Vlans allowed and active in management domain
Fa0/24      1,10,12-13,20,23,34,100,123

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1,10,12-13,20,23,34,100,123
```

```
SW2#show interfaces fastEthernet 0/24 trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/24      on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/24      1-4094

Port        Vlans allowed and active in management domain
Fa0/24      1,10,12-13,20,23-24,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1,10,12-13,20,23-24,30
```

Above you can see that the trunk is operational, we are using 802.1Q encapsulation and the native VLAN is 1. So what kind of traffic is running on the native VLAN? Let's take a look at a wireshark capture of our trunk!



As you can see some of the management protocols like CDP (Cisco Discovery Protocol) are sent on the native VLAN. For security reasons, it might be a good idea to change the native VLAN from VLAN 1 to something else. You can do it like this:

```
SW1(config)#interface fastEthernet 0/24
SW1(config-if)#switchport trunk native vlan 10
```

```
SW2(config)#interface fastEthernet 0/24
SW2(config-if)#switchport trunk native vlan 10
```

Instead of VLAN 1 we will now use VLAN 10 as the native VLAN. Let's verify our work:

```
SW1#show interfaces fastEthernet 0/24 trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/24      on               802.1q         trunking      10
```

```
SW2#show interfaces fastEthernet 0/24 trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/24      on               802.1q         trunking      10
```

There we go, VLAN 10 is now the native VLAN. Last but not least, we can also configure our switches to tag the native VLAN just like any other VLAN. Here's how to do it:

```
SW1(config)#vlan dot1q tag native
```

```
SW2(config)#vlan dot1q tag native
```

That's all there is to it! Hopefully this tutorial has been helpful to you to understand the native VLAN and how to configure it.

Configurations

Want to take a look for yourself? Here you will find the configuration of each device.

SW1

```
hostname SW1
!
interface Fastethernet 0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 10
!
vlan dot1q tag native
!
end
```

```
hostname SW2
!
interface Fastethernet 0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 10
!
vlan dot1q tag native
!
end
```

Feel free to leave a comment if you have any questions!

Rate this Lesson:

« Previous Lesson
Etherchannel over 802.1Q Tunneling

Next Lesson
VTP (VLAN Trunking Protocol) »

Home › Forums › 802.1Q Native VLAN on Cisco IOS Switch

This topic contains 36 replies, has 11 voices, and was last updated by Andrew P 1 month, 1 week ago.

Viewing 15 posts - 1 through 15 (of 37 total)
1 2 3 →

- Author
  Posts | Subscribe
- March 11, 2014 at 16:05 #12025 Reply

Rene Molenaar
Keymaster
The IEEE 802.1Q trunking protocol describes something called the “native VLAN”. All traffic sent and received on an interface that is configured for 8
[See the full post at: 802.1Q Native VLAN on Cisco IOS Switch]

March 16, 2015 at 00:43 #12026 Reply

Dan B
Participant
Is there any specific reason to tag the native vlan?

March 16, 2015 at 00:43 #12558 Reply

Dan B
Participant
Is there any specific reason to tag the native vlan?

March 16, 2015 at 10:21 #12559 Reply

Rene Molenaar
Keymaster
Hi Dan,

There is a security vulnerability (VLAN Hopping) when you don't tag the native VLAN, that's the only reason I can think of.

If you are interested, I can do a write up for VLAN hopping...might be interesting 🙂

Rene

May 17, 2015 at 23:38 #12560 Reply

Dan B
Participant
Thanks for your answer Rene, of course it would be interesting to have the write up for VLAN hopping

Regards

May 18, 2015 at 11:43 #12561 Reply

Rene Molenaar
Keymaster
Hi Dan,

I put it on my list, when it's done I'll let you know.

Rene

June 4, 2015 at 09:05 #12562 Reply

Prince
Participant
Hi René,

What is the difference between a native vlan and the default vlan ?
Are they the same ?

Thks,

June 4, 2015 at 10:49 #12563 Reply

Rene Molenaar
Keymaster
Hi Prince,

On Cisco IOS, they are the same thing. VLAN 1 is the default VLAN and it's also the native VLAN.

Rene

July 27, 2015 at 13:00 #12564 Reply

Hussein Samir
Participant
Hi Rene,

What is the benefit of changing native VLAN ? I mean what are the security reasons in detail ?
And what are the possible issues that occur because of NATIVE_VLAN_MISMATCH ?

July 27, 2015 at 13:49 #12565 Reply

Rene Molenaar
Keymaster
Hi Hussein,

An attacker would probably start looking for VLAN 1 since it's the default native VLAN. It's used for management traffic so that makes it an interesting target. It's best to use another VLAN number and to tag it for that reason.

Rene

July 27, 2015 at 19:00 #12566 Reply

Hussein Samir
Participant
Thanks Rene, I got the idea

What about second question ??

cheers.

July 27, 2015 at 19:47 #12567 Reply

Rene Molenaar
Keymaster
Ah sorry forgot about that one. A VLAN mismatch is a bad thing…

For example, if VLAN 10 is native on SW1 and VLAN 1 is native on SW2 then traffic from VLAN 10 will “leak” into VLAN 1 (or vice versa). Make sure you always use the same native VLAN on both sides of the trunk.

July 27, 2015 at 20:13 #12568 Reply

Hussein Samir
Participant
Thanks Rene, No problem.

Is there an impact on the work of STP when the NATIVE_VLAN_MISMATCH ??

July 27, 2015 at 21:16 #12569 Reply

Rene Molenaar
Keymaster
I haven’t tested it but probably the switch will report an error. PVST+ uses a bridge ID that includes the priority and vlan ID. I think STP will notice the mismatch of the VLAN ID.

October 6, 2015 at 18:18 #17846 Reply

Prince
Participant
Dear René,

Couldyou please share the link about ” vlan hopping ” if it is alreday done

Thks a lot,

Prince

- Author
  Posts

Viewing 15 posts - 1 through 15 (of 37 total)
1 2 3 →
Reply To: 802.1Q Native VLAN on Cisco IOS Switch

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

802.1Q Native VLAN on Cisco IOS Switch written by Rene Molenaar average rating 4.1/5 - 14 user ratings