**Default VLAN vs. Native VLAN**

(ref: <http://networkengineering.stackexchange.com/questions/19377/is-the-default-vlan-simply-the-default-native-untagged-vlan-on-all-interface>)

Written by Eddie (<http://networkengineering.stackexchange.com/users/3675/eddie>)

This is an often confused point for people new to the Networking, in particular to people coming up the Cisco track, due to Cisco's over emphasis on this point. It is more or less just a terminology thing. Let me explain.

The 802.1q standard defines a method of tagging traffic between two switches to distinguish which traffic belongs to which VLANs. In Cisco terms, this is what happens on a "trunk" port. I've seen other vendors refer to this as a "tagged" port. In this context, it means the same: [adding an identifier to frames](https://ciscohite.files.wordpress.com/2013/05/802.png) to indicate what VLAN the frame belongs to. Terminology aside, the main think to keep in mind is a VLAN tag is necessary, because often the traffic traversing two switches belongs to multiple VLANs, and there must be a way to determine which 1's and 0's belong to which VLAN.

But what happens if a trunk port, who is expecting to receive traffic that includes the VLAN tag, receives traffic with no tag? In the predecessor to 802.1q, known as ISL (cisco proprietary, but archaic, no one supports it anymore, not even Cisco), untagged traffic on a trunk would simply be dropped.

802.1q however, provided for a way to not only receive this traffic, but also associate it to a VLAN of your choosing. This method is known as setting a **Native VLAN**. Effectively, you configure your trunk port with a Native VLAN, and whatever traffic arrives on that port without an existing VLAN tag, gets associated to your Native VLAN.

As with all configuration items, if you do not explicitly configure something, usually some sort of default behavior exists. In the case of Cisco (and most vendors), the **Default *Native* VLAN** is VLAN 1. Which is to say, if you do not set a Native VLAN explicitly, any *untagged* traffic received on a trunk port is automatically placed in VLAN 1.

The trunk port is the "opposite" (sort of) from what is known as an **Access Port**. An access port sends and expects to receive traffic with no VLAN tag. The way this can work, is that an access port also only ever sends and expects to receive traffic *belonging to one VLAN*. The access port is statically configured for a particular VLAN, and any traffic received on that port is internally associated on the Switch itself as belonging to a particular VLAN (despite not tagging traffic for that VLAN when it leaves the switch port).

Now, to add to the confusing mix. Cisco books will often refer to the "default VLAN". The **Default VLAN** is simply the VLAN which all Access Ports are assigned to until they are explicitly placed in another VLAN. In the case of Cisco switches (and most other Vendors), the Default VLAN is usually VLAN 1. Typically, this VLAN is only relevant on an Access port, which is a port that sends and expects to receive traffic without a VLAN tag (also referred to an 'untagged port' by other vendors).

So, to summarize:

* The **Native VLAN** can change. You can set it to anything you like.
* The **Access Port VLAN** can change. You can set it to anything you like.
* The **Default Native VLAN** is always 1, this can not be change, because its set that way by Cisco
* The **Default VLAN** is always 1, this can not be changed, because it is set that way by Cisco

edit: forgot your other questions:

Also, can it / should it be changed?

This is largely an opinion question. I tend to agree with this school of thought:

All unused ports should be in a specific VLAN. All active ports should be explicitly set on to a particular VLAN. Your switch should then prevent traffic from traversing the uplink into the rest of your network if the traffic belongs on VLAN1, or the VLAN you are using for unused ports. Everything else should be allowed up the uplink.

But there are many different theories behind this. As well as differing requirements which would prevent having such a restricted switch policy (scale, resources, etc).

For instance, if a switch is going into part of a network that is only one VLAN and it's not VLAN 1, is it possible to make the "default" / native VLAN on all ports a particular VLAN using one global command, or is the preferred method to make all ports access ports and set the access VLAN to 10 on each of them?

You can not change the default Cisco configurations. You can use the "interface range" to put all ports in a different VLAN in one go. You don't really need to change the Native VLAN on the uplink trunk, so long as the other switch is using the same Native VLAN. If you really want to spare the switch from adding the VLAN Tag, you could get creative and do the following (although, its probably not recommended).

Leave all access ports in the VLAN1. Leave the Native VLAN at its default (VLAN1). On the uplink switch, set the port as a trunk port. And set its Native VLAN to the VLAN you want the lower switch to be a part of. Since the lower switch will send traffic to the upper switch untagged, the upper switch will receive it and associate it with what *it considers* the Native VLAN.