Fundamentals of 802.1Q VLAN Tagging

Virtual local area networks, or VLANs, can be used to segment traffic within a network in combination with subnetting. VLANs keep traffic from different networks separated when traversing shared links and devices within a topology. This process, also known as VLAN tagging, is invaluable to limiting broadcast network traffic and securing network segments. VLAN tagging is an integral part of networks of all sizes and is supported on MX security appliances, MR access points, and MS series switches.

- Configuring VLANs on the MX Security Appliance
- VLAN Tagging on MR Access Points

This can be done for both data and management traffic independently. For this you may refer to Understanding and Configuring Management VLANs on Cisco Meraki Devices article.

> ⓘ Best practices are to use a single subnet per VLAN ID

Common Terms

- VLAN - Virtual local area network; logical identifier for isolating a network (Understanding and Configuring VLANs)
- Trunk - A port enabled for VLAN tagging (Configuring Access and Trunk Interfaces)
- Access - A port that does not tag and only accepts a single VLAN (Configuring Access and Trunk Interfaces)
- Encapsulation - The process of modifying frames of data to include additional information
- 802.1Q - The most common encapsulation method for VLAN tagging. This is the method used by Meraki devices.
- Native VLAN - The VLAN associated with all untagged traffic on a trunk
- Subnet - A logical network that may be derived from a larger network ID

Best Practices

VLAN-enabled ports are generally categorized in one of two ways: tagged or untagged. These may also be referred to as "trunk" or "access" respectively. The purpose of a tagged or "trunked" port is to pass traffic for multiple VLANs, whereas an untagged or "access" port accepts traffic for only a single VLAN. Generally speaking, trunk ports will link switches, and access ports will link to end devices.

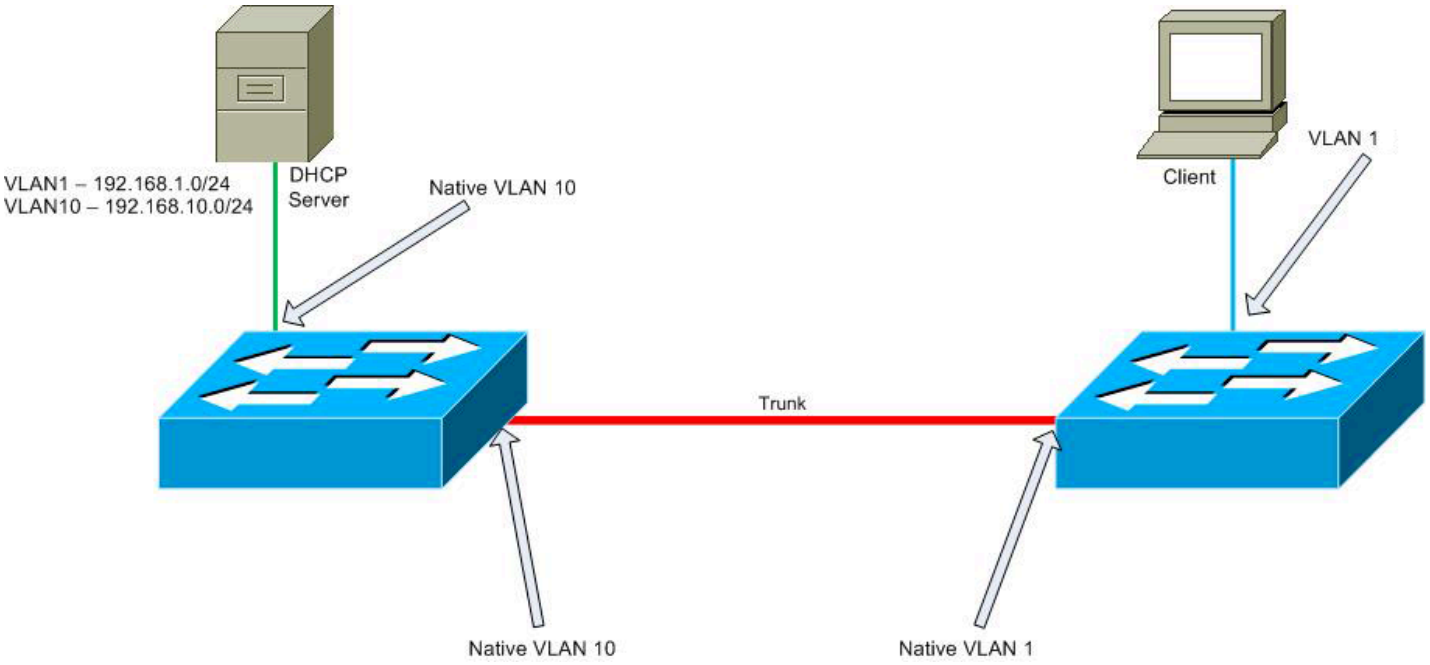
Trunk ports require more steps to successfully negotiate as a trunk.

Both ends of the link must have the following in common:

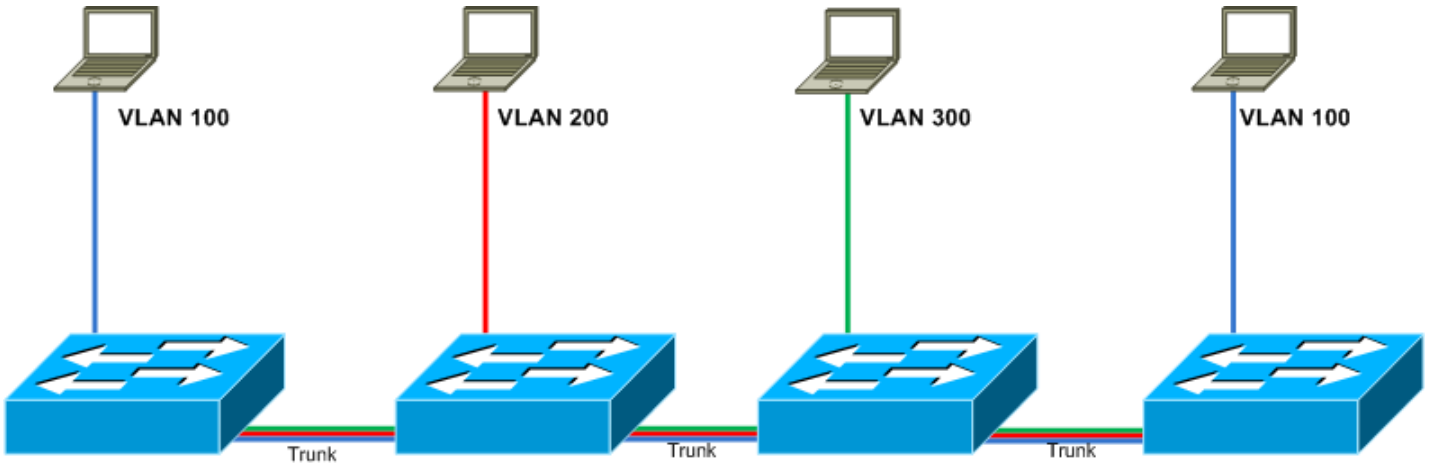
- Encapsulation
- Allowed VLANs
- Native VLAN

While a link may successfully establish with mismatched allowed or native VLANs, it is best practice to have both sides of the link configured identically. Mismatched native VLANs or allowed VLANs can have unforeseen consequences. Recall that the native VLAN is the VLAN associated with untagged traffic. Mismatched native VLANs on opposite sides of a trunk can inadvertently create "VLAN hopping." This is often a method of intentional attack used to sneak into a network and is an open security risk. Consider the following example and diagram.

A client is plugged in to a VLAN 1 access port and desires an address from the DHCP server on the VLAN 1 subnet (192.168.1.0/24). There is a native VLAN mismatch on the trunk link between the two switches, which will prevent the client from receiving the appropriate address. The DHCP request comes from the access VLAN 1 port; by the time the DHCP request gets to the trunk on the switch, it will be untagged traffic since the native VLAN is 1. When the traffic gets to the other switch on the other side of the trunk, the native VLAN is 10. The untagged traffic from the switch on the right will be treated as VLAN 10 on the switch on the left. The DHCP server will reply to the DHCP request for VLAN 10 (192.168.10.0/24) and send the address back to the client. Once again, as VLAN 10 is untagged on the left switch, it will be treated as VLAN 1 on the right switch because of the native VLAN mismatch, and the client will ultimately obtain an address in the wrong subnet.



Native VLAN setting, along with all other trunk configuration, must be identical for the entire path through the network that traffic will follow. For example, if there are three switches between a client and a gateway on VLAN 100, it must be trunked through all the switches' connecting links (shown below).



While VLANs are effective for separating network segments and limiting broadcast traffic, it is often a requirement for subnets separated by VLANs to be able to communicate. This can be accomplished only through a layer 3-enabled device that can route between the VLANs. Even if both VLANs exist on a device, their traffic will be segregated unless mediated by a layer 3 routing device.