



Meraki Implementation Note:

Using VLANs with the Meraki Enterprise Cloud Controller

May 7, 2009

This document explains how you can use VLAN tagging in conjunction with a Meraki wireless network to provide secure wireless access to multiple types of users. This tech note is designed for Meraki customers and partners.



www.meraki.com

99 Rhode Island St
San Francisco, California 94103

Phone: +1 415 632 5800
Fax: +1 415 632 5899

Copyright: © 2009 Meraki, Inc. All rights reserved.

Trademarks: Meraki® is a registered trademark of Meraki, Inc.

Table of Contents

| | | |
|----------|---|-----------|
| 1 | Introduction to VLANs..... | 4 |
| 1.1 | Meraki VLAN Support | 4 |
| 1.2 | How VLANs Work..... | 5 |
| 2 | Configuring your Wired LAN Infrastructure for Meraki | 6 |
| 2.1 | Default Behavior | 6 |
| 2.2 | VLANs and NAT | 6 |
| 2.3 | Wireless Bridging and VLANs | 7 |
| 2.4 | Testing your Configuration | 7 |
| 3 | Example Configuration..... | 8 |
| 4 | VLAN Alternative: Meraki LAN Isolation | 9 |
| 5 | Conclusion | 10 |
| 6 | Appendix: Troubleshooting..... | 11 |

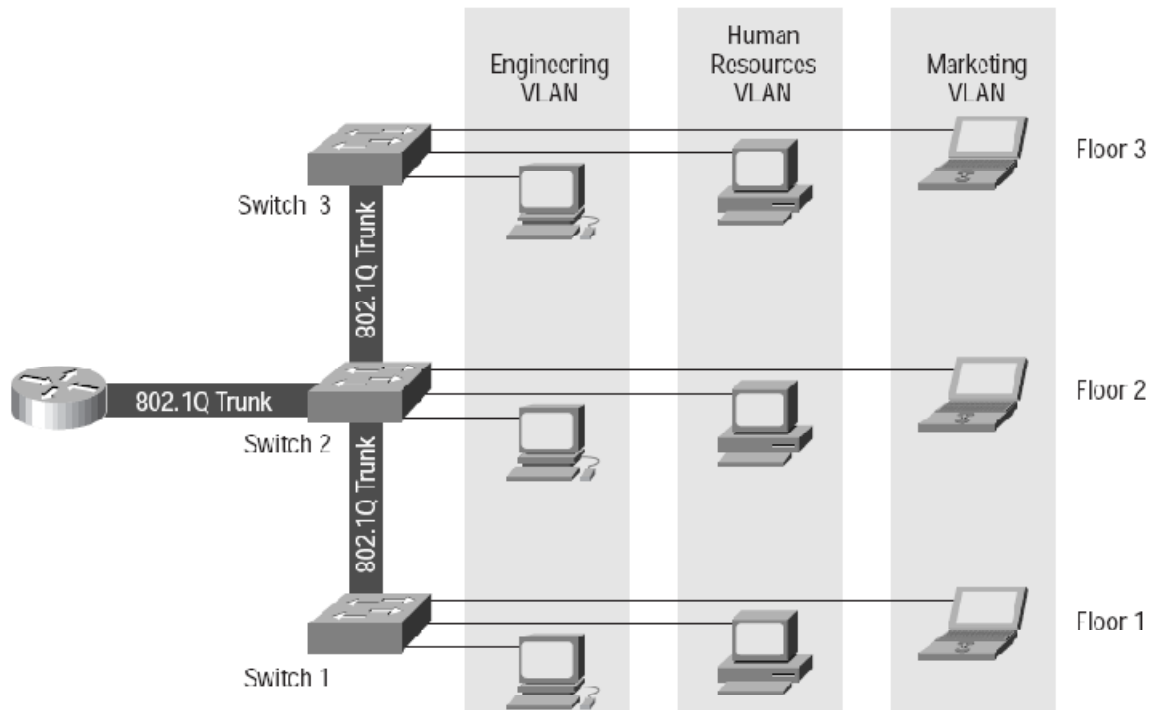
1 Introduction to VLANs

VLANs allow a single physical Ethernet network to appear to be multiple logical networks. VLANs are typically used to:

- Enhance network security by segregating client devices
- Increase performance by limiting broadcast domains

A typical VLAN configuration might break up a physical LAN by department (e.g., Engineering, HR, Marketing) or by user class (Employee, Guest). The figure below shows an example configuration.

Figure 1: Example Configuration



1.1 Meraki VLAN Support

The Meraki Enterprise Cloud Controller supports VLAN tagging, as specified in the 802.1q standard. Each Meraki Virtual Access Point (VAP) can be optionally mapped to send and receive client traffic on a specified VLAN.

1.2 How VLANs Work

A client packet is tagged with a VLAN tag when it leaves the access point and goes onto the wired network. The VLAN tag is determined by the SSID to which the client is associated, e.g., all Ethernet frames on SSID Corp might be tagged with Virtual LAN ID 10. When the AP receives a tagged packet, it will forward that packet to the correct client on any SSID that is using that VLAN ID. The AP drops all packets with VLAN IDs that do not match any of its SSID's VLAN IDs.

Meraki AP management traffic behaves somewhat differently. All packets to and from the Meraki AP are untagged. That is, they go out on the Native VLAN. As discussed below, the wired network must allow untagged packets to reach the Internet.

2 Configuring your Wired LAN Infrastructure for Meraki

The Meraki system is designed to minimize the changes you need to make to your wired infrastructure. However, there are requirements that must be met:

1. Each Meraki AP must be plugged into a VLAN trunk port.
2. Untagged traffic on the AP trunk ports must be allowed out to the Internet.
3. The trunk port to which the AP is connected must have access to all VLANs in use in the wireless network.

If you are using VLANs for security, Meraki recommends that no SSID be assigned to the Native (untagged) VLAN.

If you have a LAN with a lot of broadcast traffic, you may want to consider limiting the VLANs that are visible on the Meraki-attached trunk port. This will reduce the amount of broadcast traffic that the Meraki AP sees, increasing performance in some cases.

The Meraki Enterprise Cloud Controller supports up to four virtual access points/SSIDs. A VLAN can be assigned to one or more SSIDs.

2.1 Default Behavior

If you do not specify a VLAN ID for a VAP, client traffic will be untagged by default and therefore be sent on the Native VLAN.

2.2 VLANs and NAT

Most Meraki networks in a corporate setting use Bridge Mode, in which clients receive the IP address from the corporate DHCP server and the WLAN appears to be an extension of the LAN. Meraki also supports NAT Mode, in which all wireless clients DHCP from the access point and receive an address from a private address space. NAT may be enabled on a per-virtual-access-point basis.

VLAN tagging cannot be used on SSIDs that are using NAT mode. All client traffic from a NAT mode SSID is sent from the AP's IP address, which always sends untagged traffic.

2.3 Wireless Bridging and VLANs

A wireless bridge might be used to connect two buildings that do not have a wired connection. For example, one might have:

Internet – LAN 1 – AP1 – wireless link – AP2 – LAN2

AP1 and AP2 form a wireless bridge between LAN1 and LAN 2. Meraki does not support wireless bridging. Please see your Meraki sales representative if you have a need to use VLAN tagging in a wireless bridge scenario.

2.4 Testing your Configuration

VLAN configuration can be complex, so it is important to test your network thoroughly before moving it into production. The following procedure is a guide to ensuring you have configured your network properly.

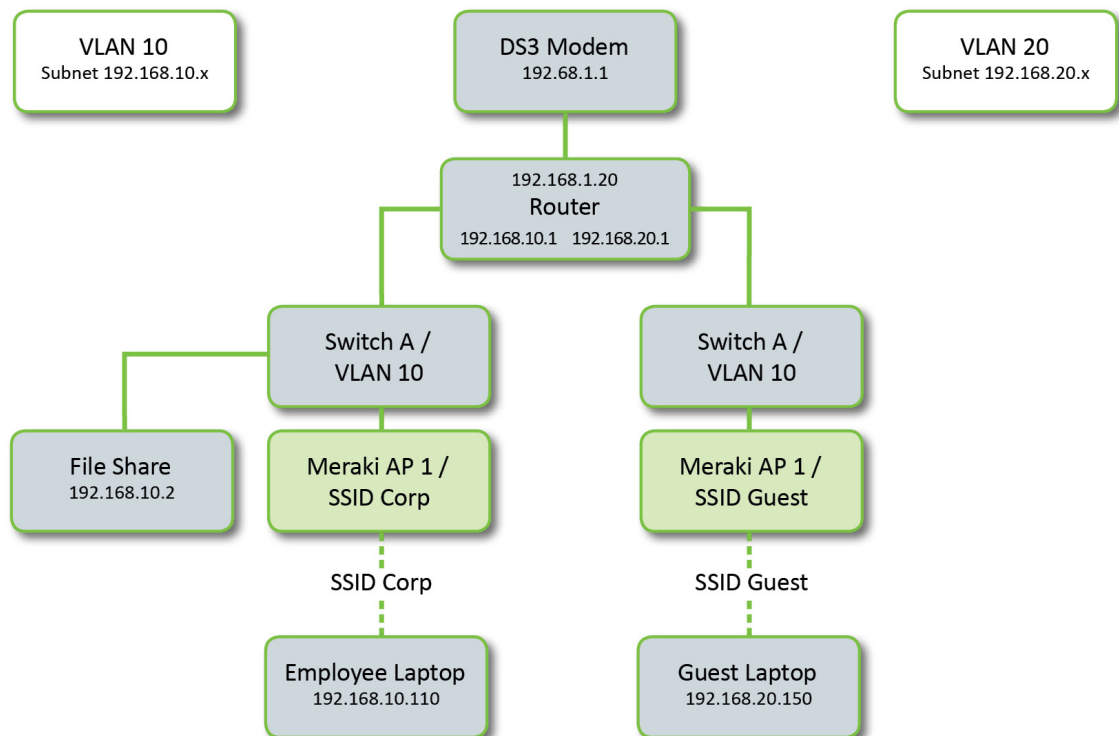
1. Ensure that the test AP can reach the internet. You can do this by going to Dashboard and pinging each AP.
2. Associate as a client on one of your SSIDs. Ensure ping behavior works as expected for:
 - i. A device on the same VLAN
 - ii. A device on a different VLAN that is supposed to be reachable
 - iii. A device on a different VLAN that is not supposed to be reachable
 - iv. The Internet (if the VLAN is supposed to have Internet access)

3 Example Configuration

The following diagram depicts a typical corporate architecture using VLANs with wireless access points. The network has two VLANs, 10 and 20. VLAN 10 is for employee use, while VLAN 20 is for guest use.

Switch A is shown twice because it is logically two switches. However, there is only one physical switch A. Meraki AP 1 is also shown twice because it is logically two access points (SSID Corp and SSID Guest). However, there is only one physical access point.

Figure 2: Logical Network Architecture



The desired behavior of the network is that employee traffic can access all LAN resources, while guest traffic can only access the Internet. In order to achieve this behavior, the router must be configured to allow both VLAN 10 and VLAN 20 to access the Internet, but not directly communicate with one another.

As a side benefit, broadcast traffic on the employee network does not reach the guest network, and visa versa.

4 VLAN Alternative: Meraki LAN Isolation

Meraki also supports a feature called “LAN Isolation” which, in some situations, can eliminate the need to use VLAN tagging with your wireless network. LAN Isolation, which can be enabled on a per-VAP basis, prevents client traffic from accessing the LAN. LAN addresses are those in the following IP ranges:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

One advantage of using Meraki LAN Isolation is that it requires no changes to your existing wired infrastructure, and is also very easy to set up and maintain.

5 Conclusion

VLAN tagging / 802.1Q can help make your wireless networks more secure and allow you to serve multiple user groups and applications on the same wired infrastructure. Meraki fully supports VLAN tagging on a per-VAP/SSID basis.

6 Appendix: Troubleshooting

The following section provides basic troubleshooting tips. For additional assistance, see the Meraki Knowledge Base.

Symptom: Clients cannot access the LAN or the Internet but access points are alive on Dashboard.

- Ensure your switches are configured to allow the chosen VLANs to access the LAN and/or the Internet.
- Ensure that the AP trunk port is allowed to send frames with all of the VLANs you have in use.
- Most of the time you can verify that the switch port to which the AP is connected is correctly configured by plugging in a laptop and running a packet capture program. You should see broadcast packets that have 802.1Q VLAN headers from the VLANs that clients are configured to use. If you do not see these VLAN headers, then the port is probably not configured as a trunk port.

Symptom: Your access points are not showing up on Meraki Dashboard.

- Ensure that each AP is plugged into a trunk port.
- Ensure that the AP is plugged into a port that has a native VLAN assigned, and that the native VLAN has the appropriate permissions to access the internet. This can generally be tested by plugging in a laptop instead of the AP into the port, and verifying that the laptop can reach the internet.