# Comparing Layer 3 and Layer 2 Switches

This article outlines the difference between layer 2 and layer 3 switches and the appropriate use cases for each.

Learn more with this free online training course on the Meraki Learning Hub:
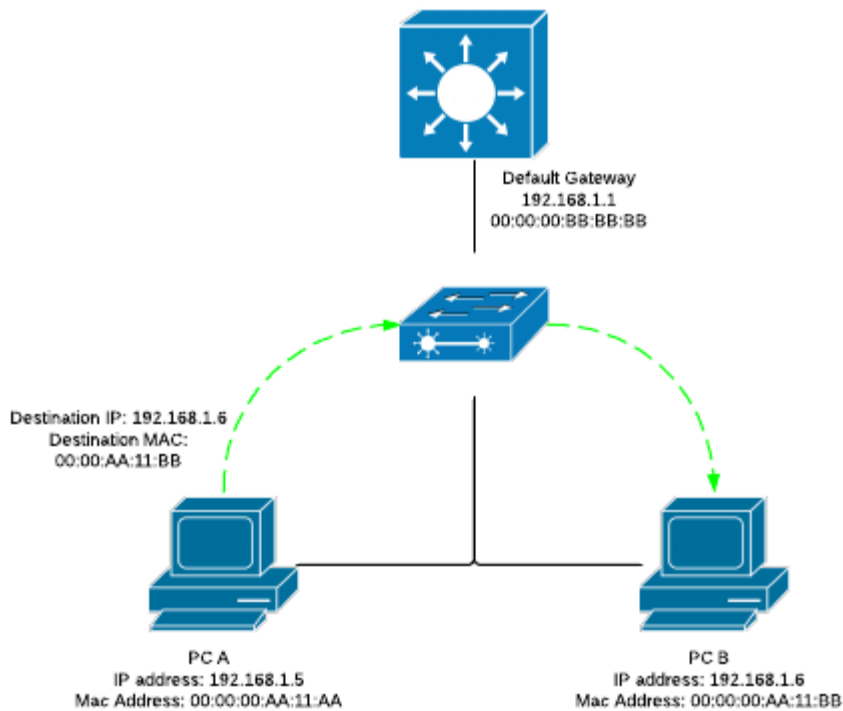
- Configuring Layer 3 Routing

Sign in with your Cisco SSO or create a free account to start training.

Traditional switching operates at layer 2 of the Open Systems Interconnection (OSI) model, where packets are sent to a specific switch port based on destination MAC addresses. Routing operates at layer 3, where packets are sent to a specific next-hop IP address based on the destination IP address. Devices in the same layer 2 segment do not need routing to reach local peers. However, the destination MAC address is needed. It can be resolved through the Address Resolution Protocol (ARP) as illustrated below:
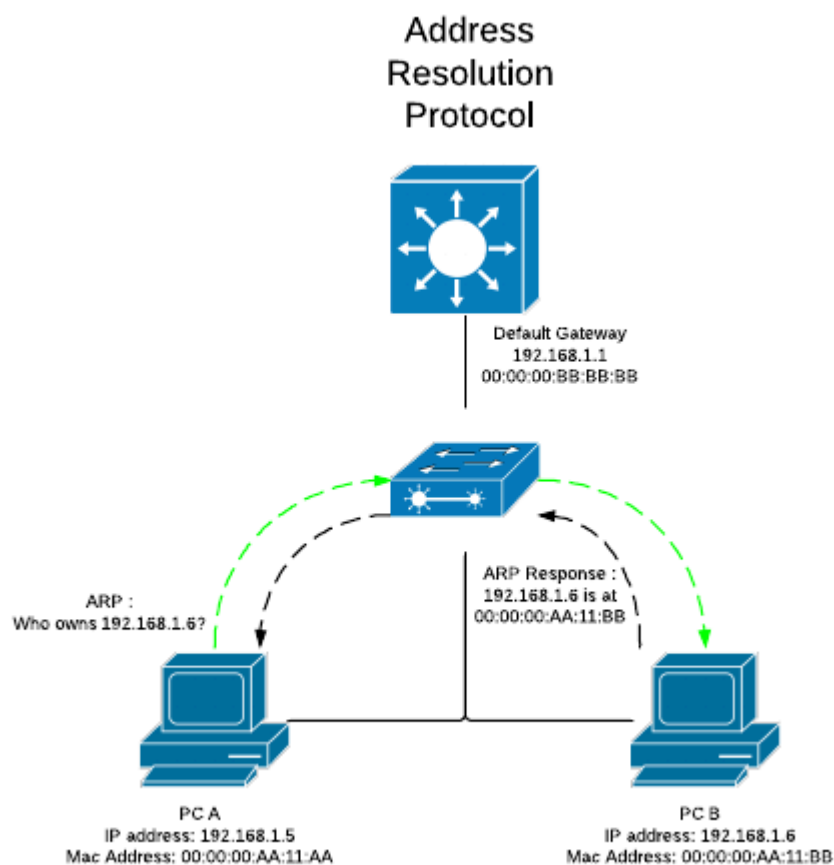
In the diagram above, PC A wants to send traffic to PC B at IP address 192.168.1.6. It does not know the unique MAC address until it discovers it through an ARP, which is broadcasted throughout the layer 2 segment.

Layer 2 Switching

Default Gateway
192.168.1.1
00:00:00:BB:BB:BB

Destination IP: 192.168.1.6
Destination MAC:
00:00:AA:11:BB

PC A
IP address: 192.168.1.5
Mac Address: 00:00:00:AA:11:AA

PC B
IP address: 192.168.1.6
Mac Address: 00:00:00:AA:11:BB

Then, it sends the packet to the appropriate destination MAC address. After that, the switch will forward out the correct port based on its MAC-Address-Table.

Within a layer 2 switch environment exists a broadcast domain. Any broadcast traffic on a switch will be forwarded out to all ports except for the port the broadcast packet arrived on. Broadcasts are contained in the same layer 2 segment, as they do not traverse past a layer 3 boundary.
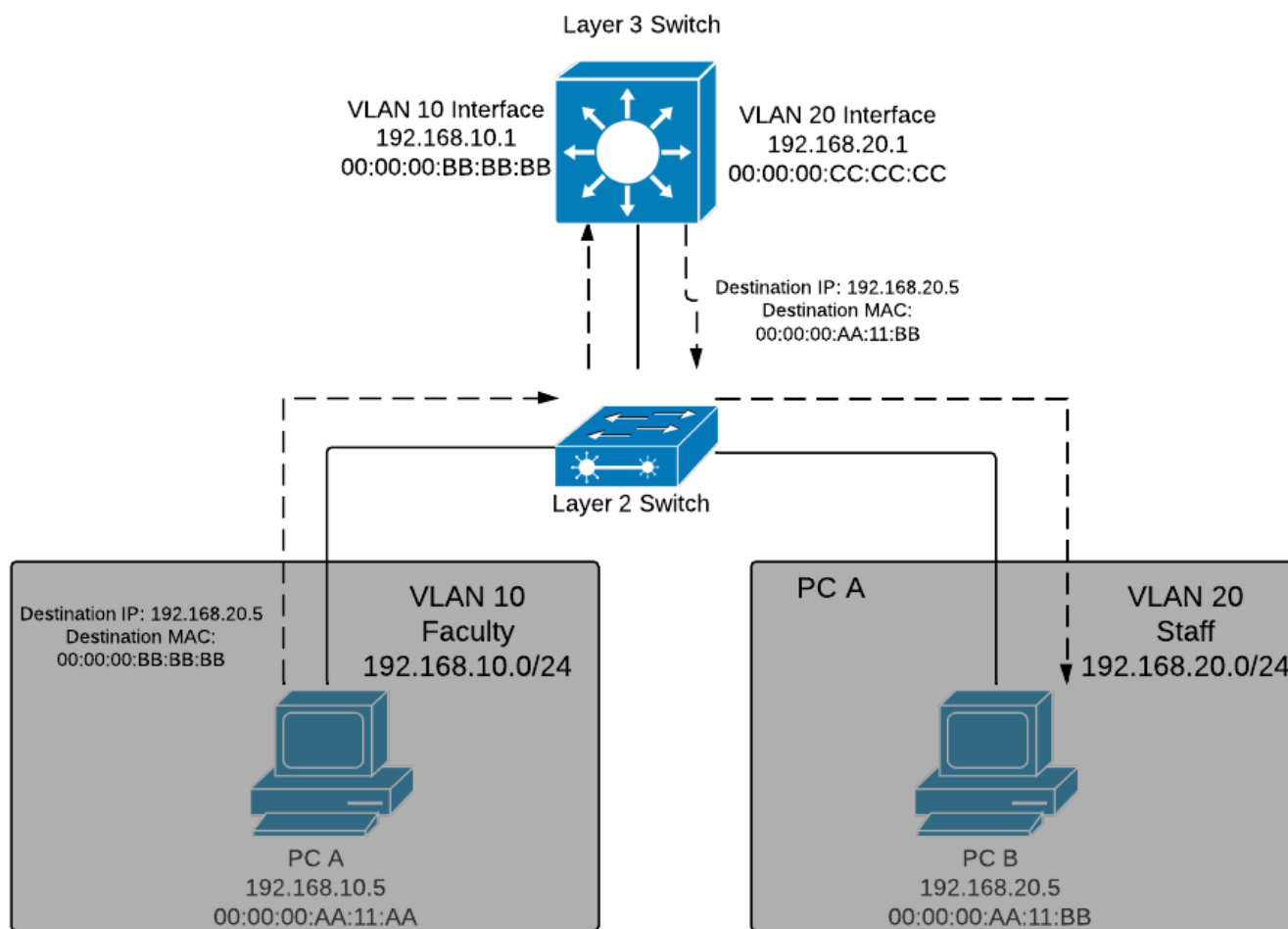
Large layer 2 broadcast domains can be susceptible to problems, like broadcast storms, which can cause network outages. Also, for security and policy reasons, it is best to separate certain clients into different broadcast domains. This is when it becomes useful to configure VLANs. In turn, the switch ports are in different layer 3 subnets and different broadcast domains. VLANs allow for greater flexibility by allowing different layer 3 networks to be sharing the same layer 2 infrastructure. The image below shows an example of a multi-VLAN environment on a layer 2 switch:
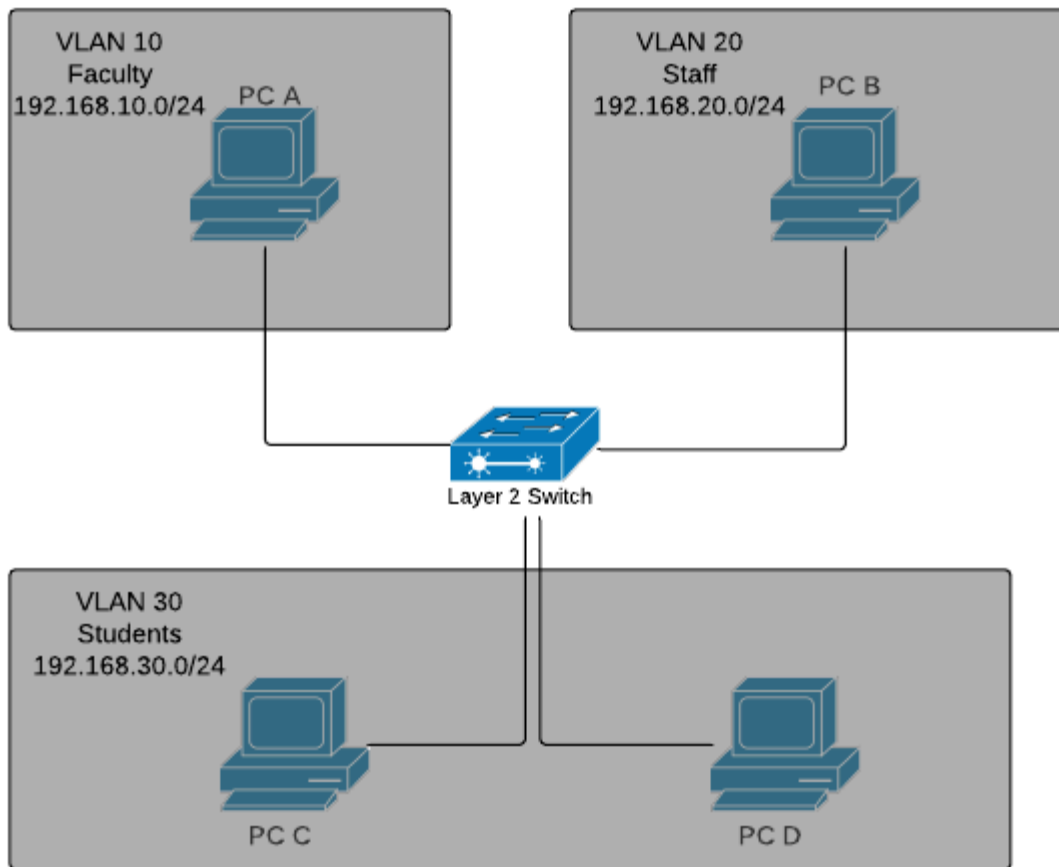
Since VLANs exist in their own layer 3 subnet, routing will need to occur for traffic to flow in between VLANs. This is where a layer 3 switch can be utilized. A Layer 3 switch is basically a switch that can perform routing functions in addition to switching. A client computer requires a default gateway for layer 3 connectivity to remote subnets. When the computer sends traffic to another subnet, the destination MAC address in the packet is for the default gateway. Then, the gateway will accept the packet at layer 2 and proceed to route the traffic to the destination based on its routing table.

The diagram below shows an example of a layer 3 switch routing between VLANs through its two VLAN interfaces. As before, the layer 3 device will still need to resolve the MAC address of PC B through an ARP request broadcasted out to VLAN 20. It then rewrites the appropriate destination MAC address and forwards the packet back out the layer 2 segment:

Inter-VLAN Routing

Layer 3 Switch

VLAN 10 Interface
192.168.10.1
00:00:00:BB:BB:BB

VLAN 20 Interface
192.168.20.1
00:00:00:CC:CC:CC

Destination IP: 192.168.20.5
Destination MAC:
00:00:00:AA:11:BB

Layer 2 Switch

Destination IP: 192.168.20.5
Destination MAC:
00:00:00:BB:BB:BB

VLAN 10
Faculty
192.168.10.0/24

PC A

PC A
192.168.10.5
00:00:00:AA:11:AA

VLAN 20
Staff
192.168.20.0/24

PC B
192.168.20.5
00:00:00:AA:11:BB

Additional Resources

MS Layer 3 Switching and Routing: An overview of how to configure layer 3 routing on Cisco Meraki switches

Layer 3 Switch Example: A configuration example using layer 3 routing on Cisco Meraki switches

Fundamentals of 802.1Q VLAN Tagging: Information regarding the appropriate use of VLAN tags