In today’s complex enterprise networks comprising many subnets and virtual LANs, a layer 3 switch plays an important role in many systems. But do you need this in your network? Let’s see.

**What is a layer 3 switch?**

Simply put, a layer 3 switch combines the functionality of a switch and a router. It acts as a switch to connect devices that are on the same subnet or virtual LAN at lightning speeds and has IP routing intelligence built into it to double up as a router. It can support routing protocols, inspect incoming packets, and can even make routing decisions based on the source and destination addresses. This is how a layer 3 switch acts as both a switch and a router.

Often referred to as a multilayer switch, a layer 3 switch adds a ton of flexibility to a network.

**Features of a layer 3 switch**

The features of a layer 3 switch are:

* Comes with 24 Ethernet ports, but no WAN interface.
* Acts as a switch to connect devices within the same subnet.
* Switching algorithm is simple and is the same for most routed protocols.
* Performs on two [OSI layers](http://techgenix.com/network-troubleshooting-osi/) — layer 2 and layer 3.

**Purpose of a layer 3 switch**

There is a ton of confusion about the use of a layer 3 switch because in a traditional setup, routers operate at layer 3 of the OSI model while switches operate at layer 2. So, how does this layer 3 switch fit into this model? Also, the name “layer 3 switch” causes confusion because switches typically operate from layer 2.

Originally, layer 3 switches were conceived to improve routing performance on large networks, especially corporate intranets. To understand the purpose, let’s step back a bit in time to see how these switches evolved.

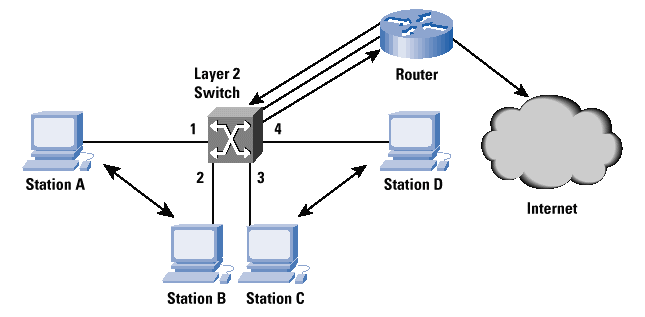
[Layer 2 switches](https://www.techopedia.com/definition/8011/layer-2-switch) work well when there is low to medium traffic in VLANs. But these switches would hang when traffic increased. So, it became necessary to augment layer 2’s functionality.

One option was to use a router instead of a switch, but then routers are slower than switches, so this could lead to slower performance.

To overcome this downside, researchers thought about implementing a router within a switch. Though technically feasible, it was not the ideal option because [layer 2](http://techgenix.com/layer-2-external-access-cisco-aci/) switches operate only on the Ethernet MAC frame while layer 3 handles multiple routing protocols.

Researchers felt this was too complicated, so they came up with the idea of a layer 3 switches that acted as routers with fast forwarding done through the underlying hardware.

This is why the main difference between layer 3 switches and routers lies in the hardware. If you were to take a peek into a layer 3 switch’s hardware, you’ll see a mix of traditional switches and routers, except that the routers’ software logic is replaced with integrated circuit hardware to improve performance.



Cisco

Also, a layer 3 switch’s router will not have WAN ports and other WAN features you’ll typically see in a traditional router.

**Benefits of a layer 3 switch**

From the above discussion, the purpose/benefits of a layer 3 switch are to:

* Support routing between virtual LANs.
* Improve fault isolation.
* Simplify security management.
* Reduce broadcast traffic volumes.
* Ease the configuration process for VLANs, as a separate router isn’t required between each VLAN.
* Separate routing tables, and as a result, segregate traffic better.
* Simplify troubleshooting as, fixing problems in L2 layer is tedious and time-consuming.
* Support flow accounting and high-speed scalability.
* Lower network latency as a packet doesn’t have to make extra hops to go through a router.

Now that you know why your organization needs a layer 3 switch, let’s also look at the potential problems that come with it.

**Disadvantages of layer 3 switch**

Just like any product, a layer 3 switch also comes with its own share of downsides. We’ll briefly look into each of these disadvantages to help you make the right decision.

**Cost**

Cost is one of the major downsides to a layer 3 switch. It costs much more than a traditional switch and configuring and administering these switches also requires more effort. So, an organization should be ready to spend extra resources to set up layer 3 switches.

**Limited application**

Layer 3 switches are most applicable only for large intranet environments with many device subnets and traffic. Homes and small organizations do not need these switches.

**Lack of WAN functionality**



Lack of WAN functionality is another major disadvantage with layer 3 switches. This means you can’t do away with routers completely and you’ll need both routers and layer 3 switches for routing traffic within and outside your organization.

**Multiple tenants and virtualization**

When compared to layer 2 switching, layer 3 routing is relatively slower. This can be an issue when you want to span VLAN over multiple switches for supporting multiple tenants and virtualization.

**Lack of flexibility**

Since you’re routing at the access layer, [VLANs](http://techgenix.com/creating-vlan-pools-and-layer-2-bridge-domains-cisco-application-centric-infrastructure/) will be local to that specific switch. In other words, one VLAN will be associated with one switch and can’t be used on other switches. This limitation means you have to plan well to avoid one LAN from using multiple switches.

**Do you need it?**

Now comes the big question: Do you need a layer 3 switch at all for your network? Well, it depends on your network configuration and its size.

Generally speaking, you need a layer 3 switch if you answer yes to any of the below questions.

* Do you have VLANs in your network? Are you planning to include them in the near future?
* Do individual departments need separate broadcast domains for security and performance?
* Do you have subnets connected through a router?
* Does your network have more than 250 devices connected to the same VLAN?

If you answered yes to one or more of the above questions, you sure need a layer 3 switch for improved performance. In all other cases, it is optional.

Layer 3 switches act as both switches and routers. They are ideal for VLANs only, as they do not have a WAN interface. But within VLANs, it gives you multiple options to manage your bandwidth efficiently. This is why layer 3 switches are a powerful and scalable technology for building high-performance Ethernets.

Have you implemented a layer 3 switch in your organization? Can you please share your experience with our readers in the comments section?

# Multilayer switch

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Multilayer_switch#mw-head) [Jump to search](https://en.wikipedia.org/wiki/Multilayer_switch#searchInput)

|  |  |
| --- | --- |
|  | This article **needs additional citations for** [**verification**](https://en.wikipedia.org/wiki/Wikipedia:Verifiability). Please help [improve this article](https://en.wikipedia.org/w/index.php?title=Multilayer_switch&action=edit) by [adding citations to reliable sources](https://en.wikipedia.org/wiki/Help:Referencing_for_beginners). Unsourced material may be challenged and removed. *Find sources:* ["Multilayer switch"](https://www.google.com/search?as_eq=wikipedia&q=%22Multilayer+switch%22) – [news](https://www.google.com/search?tbm=nws&q=%22Multilayer+switch%22+-wikipedia) **·** [newspapers](https://www.google.com/search?&q=%22Multilayer+switch%22+site:news.google.com/newspapers&source=newspapers) **·** [books](https://www.google.com/search?tbs=bks:1&q=%22Multilayer+switch%22+-wikipedia) **·** [scholar](https://scholar.google.com/scholar?q=%22Multilayer+switch%22) **·** [JSTOR](https://www.jstor.org/action/doBasicSearch?Query=%22Multilayer+switch%22&acc=on&wc=on) *(October 2009) (*[*Learn how and when to remove this template message*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)* |

|  |  |
| --- | --- |
|  | It has been suggested that portions of [*Network switch#Layer-specific functionality*](https://en.wikipedia.org/wiki/Network_switch#Layer-specific_functionality) be [split](https://en.wikipedia.org/wiki/Wikipedia:Splitting) from it and [merged](https://en.wikipedia.org/wiki/Wikipedia:Merging) into this article. ([Discuss](https://en.wikipedia.org/wiki/Talk:Network_switch#Merge_from_LAN_switching)) *(July 2018)* |

A **multilayer switch (MLS)** is a [computer networking device](https://en.wikipedia.org/wiki/Computer_networking_device) that switches on [OSI layer 2](https://en.wikipedia.org/wiki/Data_link_layer) like an ordinary [network switch](https://en.wikipedia.org/wiki/Network_switch) and provides extra functions on higher [OSI layers](https://en.wikipedia.org/wiki/OSI_model).

Switching technologies are crucial to [network design](https://en.wikipedia.org/wiki/Network_design), as they allow traffic to be sent only where it is needed in most cases, using fast, hardware-based methods. Switching uses different kinds of [network switches](https://en.wikipedia.org/wiki/Network_switch). A standard switch is known as a *layer 2 switch* and is commonly found in nearly any LAN. *Layer 3* or *layer 4* switches require advanced technology (see [managed switch](https://en.wikipedia.org/wiki/Network_switch#Configuration_options)) and are more expensive, and thus are usually only found in larger LANs or in special network environments.



## Contents

* [1 Multilayer switch](https://en.wikipedia.org/wiki/Multilayer_switch#Multilayer_switch)
* [2 Layer 2 switching](https://en.wikipedia.org/wiki/Multilayer_switch#Layer_2_switching)
* [3 Layer-3 switching](https://en.wikipedia.org/wiki/Multilayer_switch#Layer-3_switching)
* [4 Layer 4 switching](https://en.wikipedia.org/wiki/Multilayer_switch#Layer_4_switching)
  + [4.1 Layer 4–7 switch, web switch, or content switch](https://en.wikipedia.org/wiki/Multilayer_switch#Layer_4–7_switch,_web_switch,_or_content_switch)
  + [4.2 Layer 4 load balancer](https://en.wikipedia.org/wiki/Multilayer_switch#Layer_4_load_balancer)
* [5 See also](https://en.wikipedia.org/wiki/Multilayer_switch#See_also)
* [6 References](https://en.wikipedia.org/wiki/Multilayer_switch#References)
* [7 External links](https://en.wikipedia.org/wiki/Multilayer_switch#External_links)

## Multilayer switch

Multi-layer switching combines layer 2, 3 and 4 switching technologies and provides high-speed scalability with low latency. Multi-layer switching can move traffic at wire speed and also provide layer 3 routing. There is no performance difference between forwarding at different layers because the routing and switching is all hardware based – routing decisions are made by specialized [ASIC](https://en.wikipedia.org/wiki/Application-specific_integrated_circuit) with the help of [content-addressable memory](https://en.wikipedia.org/wiki/Content-addressable_memory).[[1]](https://en.wikipedia.org/wiki/Multilayer_switch#cite_note-switchoperation-1)

Multi-layer switching can make routing and switching decisions based on the following

* [MAC address](https://en.wikipedia.org/wiki/MAC_address) in a data link frame
* Protocol field in the data link frame
* IP address in the [network layer](https://en.wikipedia.org/wiki/Network_layer) header
* Protocol field in the network layer header
* Port numbers in the [transport layer](https://en.wikipedia.org/wiki/Transport_layer) header

MLSs implement [QoS](https://en.wikipedia.org/wiki/Quality_of_service) in hardware. A multilayer switch can prioritize [packets](https://en.wikipedia.org/wiki/Packet_(information_technology)) by the 6 bit [differentiated services code point](https://en.wikipedia.org/wiki/Differentiated_services_code_point) (DSCP). These 6 bits were originally used for [type of service](https://en.wikipedia.org/wiki/Type_of_service). The following 4 mappings are normally available in an MLS:[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

* From OSI layer 2, 3 or 4 to IP DSCP (for IP packets) or [IEEE 802.1p](https://en.wikipedia.org/wiki/IEEE_802.1p)
* From IEEE 802.1p to IP DSCP
* From IP DSCP to IEEE 802.1p
* From VLAN IEEE 802.1p to port egress queue.

MLSs are also able to route IP traffic between [VLANs](https://en.wikipedia.org/wiki/VLAN) like a common [router](https://en.wikipedia.org/wiki/Router_(computing)). The routing is normally as quick as switching (at [wire speed](https://en.wikipedia.org/wiki/Wire_speed)).

## Layer 2 switching

[Layer-2](https://en.wikipedia.org/wiki/Layer_2) switching uses the [MAC address](https://en.wikipedia.org/wiki/MAC_address) of the host's [network interface cards](https://en.wikipedia.org/wiki/Network_interface_card) (NICs) to decide where to forward frames. Layer 2 switching is hardware-based, which means switches use [application-specific integrated circuit](https://en.wikipedia.org/wiki/Application-specific_integrated_circuit) (ASICs) to build and maintain the [Forwarding information base](https://en.wikipedia.org/wiki/Forwarding_information_base) and to perform [packet forwarding](https://en.wikipedia.org/wiki/Packet_forwarding) at wire speed. One way to think of a layer-2 switch is as multiport [bridge](https://en.wikipedia.org/wiki/Bridging_(networking)).

Layer-2 switching is highly efficient because there is no modification to the frame required. Encapsulation of the packet changes only when the data packet passes through dissimilar media (such as from Ethernet to FDDI). Layer-2 switching is used for workgroup connectivity and network segmentation (breaking up [collision domains](https://en.wikipedia.org/wiki/Collision_domain)). This allows a flatter network design with more network segments than traditional networks joined by [repeater hubs](https://en.wikipedia.org/wiki/Repeater_hub) and routers.

Layer-2 switches have the same limitations as bridges. Bridges break up collision domains, but the network remains one large [broadcast domain](https://en.wikipedia.org/wiki/Broadcast_domain) which can cause performance issues and limits the size of a network. Broadcast and multicasts, along with the slow convergence of spanning tree, can cause major problems as the network grows. Because of these problems, layer-2 switches cannot completely replace routers. Bridges are good if a network is designed by the [80/20 rule](https://en.wikipedia.org/wiki/Pareto_principle): users spend 80 percent of their time on their local segment.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

## Layer-3 switching

Layer-3 switching is solely based on (destination) [IP address](https://en.wikipedia.org/wiki/IP_address) stored in the header of [IP datagram](https://en.wikipedia.org/wiki/Datagram) (layer-4 switching may use other information in the header). The difference between a layer-3 switch and a router is the way the device is making the routing decision. Traditionally, routers use microprocessors to make forwarding decisions in software, while the switch performs only hardware-based packet switching (by specialized [ASIC](https://en.wikipedia.org/wiki/Application-specific_integrated_circuit) with the help of [content-addressable memory](https://en.wikipedia.org/wiki/Content-addressable_memory)).[[1]](https://en.wikipedia.org/wiki/Multilayer_switch#cite_note-switchoperation-1)[[2]](https://en.wikipedia.org/wiki/Multilayer_switch#cite_note-2) However, many routers now also have advanced hardware functions to assist with forwarding.

The main advantage of layer-3 switches is the potential for lower network [latency](https://en.wikipedia.org/wiki/Latency_(engineering)) as a packet can be routed without making extra network hops to a router. For example, connecting two distinct segments (e.g. [VLANs](https://en.wikipedia.org/wiki/Virtual_LAN)) with a router to a standard layer-2 switch requires passing the frame to the switch (first L2 hop), then to the router (second L2 hop) where the packet inside the frame is routed (L3 hop) and then passed back to the switch (third L2 hop). A layer-3 switch accomplishes the same task without the need for a router (and therefore additional hops) by making the routing decision itself, i.e. the packet is routed to another subnet and switched to the destination network port simultaneously.

Because many layer-3 switches offer the same functionality as traditional routers they can be used as cheaper, lower latency replacements in some networks. Layer 3 switches can perform the following actions that can also be performed by routers:

* determine paths based on [logical addressing](https://en.wikipedia.org/wiki/Logical_address)
* check and recompute layer-3 header [checksums](https://en.wikipedia.org/wiki/Checksum)
* examine and update [time to live](https://en.wikipedia.org/wiki/Time_to_live) (TTL) field
* process and respond to any option information
* update [Simple Network Management Protocol](https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol) (SNMP) managers with [Management Information Base](https://en.wikipedia.org/wiki/Management_Information_Base) (MIB) information

The benefits of layer 3 switching include the following:

* fast hardware-based packet forwarding with low latency
* lower per-port cost compared to pure routers
* flow accounting
* [Quality of service](https://en.wikipedia.org/wiki/Quality_of_service) (QoS)

IEEE[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] has developed hierarchical terminology that is useful in describing forwarding and switching processes. Network devices without the capability to forward packets between subnetworks are called end systems (ESs, singular ES), whereas network devices with these capabilities are called intermediate systems (ISs). ISs are further divided into those that communicate only within their routing domain (intradomain IS) and those that communicate both within and between routing domains (interdomains IS). A routing domain is generally considered as portion of an internetwork under common administrative authority and is regulated by a particular set of administrative guidelines. Routing domains are also called autonomous systems.

## Layer 4 switching

Layer 4 switching means hardware-based layer 3 switching technology that can also consider the type of network traffic (for example, distinguishing between [UDP](https://en.wikipedia.org/wiki/User_Datagram_Protocol) and [TCP](https://en.wikipedia.org/wiki/Transmission_Control_Protocol)). Layer 4 switching provides additional datagram inspection by reading the [port numbers](https://en.wikipedia.org/wiki/Port_number) found in the transport layer header to make routing decisions (i.e. ports used by [HTTP](https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol), [FTP](https://en.wikipedia.org/wiki/File_Transfer_Protocol) and [VoIP](https://en.wikipedia.org/wiki/Voice_over_IP)). These port numbers are found in [RFC 1700](https://tools.ietf.org/html/rfc1700) and reference the upper-layer protocol, program, or application.

Using layer-4 switching, the network administrator can configure a layer-4 switch to prioritize data traffic by application. Layer-4 information can also be used to help make routing decisions. For example, extended access lists can filter packets based on layer-4 port numbers. Another example is accounting information gathered by open standards using [sFlow](https://en.wikipedia.org/wiki/SFlow).

### Layer 4–7 switch, web switch, or content switch

Some switches can use up to OSI layer 7 packet information; these may be called layer 4–7 switches, [content switches](https://en.wikipedia.org/wiki/Content_switch), content services switches, web switches or application switches.

Content switches are typically used for [load balancing](https://en.wikipedia.org/wiki/Load_balancer) among groups of servers. Load balancing can be performed on [HTTP](https://en.wikipedia.org/wiki/HTTP), [HTTPS](https://en.wikipedia.org/wiki/HTTPS), [VPN](https://en.wikipedia.org/wiki/VPN), or any TCP/IP traffic using a specific port. Load balancing often involves [destination network address translation](https://en.wikipedia.org/wiki/Destination_network_address_translation) so that the client of the load balanced service is not fully aware of which server is handling its requests. Some of the layer 4–7 switches can perform [NAT](https://en.wikipedia.org/wiki/Network_Address_Translation) at wirespeed. Also, content switches can often be used to perform standard operations such as [SSL](https://en.wikipedia.org/wiki/Secure_Sockets_Layer) encryption/decryption to reduce the load on the servers receiving the traffic, or to centralise the management of [digital certificates](https://en.wikipedia.org/wiki/Digital_certificate). Layer 7 switching is the base technology of a [content delivery network](https://en.wikipedia.org/wiki/Content_delivery_network).[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

Some types of applications require that repeated requests from a client are directed at the same application server. Since the client isn't generally aware of which server it spoke to earlier, content switches define a notion of stickiness. For example, requests from the same source IP address are directed to the same application server each time. Stickiness can also be based on [SSL](https://en.wikipedia.org/wiki/Secure_Sockets_Layer) IDs, and some content switches can even use [cookies](https://en.wikipedia.org/wiki/HTTP_cookie) to provide this functionality.

### Layer 4 load balancer

A typical network router simply sends incoming packets onto the appropriate [IP address](https://en.wikipedia.org/wiki/IP_address) on its network. A [*layer 4*](https://en.wikipedia.org/wiki/Layer_4) *router*, more correctly a NAT with port and transaction awareness, usually performs a form of [port translation](https://en.wikipedia.org/wiki/Port_translation) for sending incoming packets to one or more machines that are hidden behind a single IP address.

The "layer 4" refers to the layer 4 or [transport layer](https://en.wikipedia.org/wiki/Transport_layer) of the [OSI model](https://en.wikipedia.org/wiki/OSI_model). The router operates on the [transport layer](https://en.wikipedia.org/wiki/Transport_layer) and makes decisions on where to send the packets. Modern [load balancing](https://en.wikipedia.org/wiki/Load_balancing_(computing)) routers can use different rules to make decisions on where to route traffic. This can be based on least load, or fastest [response times](https://en.wikipedia.org/wiki/Response_time_(technology)), or simply balancing requests out. This is also a [redundancy](https://en.wikipedia.org/wiki/Redundancy_(engineering)) method, so if one machine is not up, the router will not send traffic to it.

## See also

* [Application delivery controller](https://en.wikipedia.org/wiki/Application_delivery_controller)
* [Bridge router](https://en.wikipedia.org/wiki/Bridge_router)
* [Multiprotocol Label Switching (MPLS)](https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching)
* [Residential gateway](https://en.wikipedia.org/wiki/Residential_gateway)

## References

 Hucaby, David (Oct 24, 2003). [*"Switch Operation for the CCNP BCMSN Exam"*](http://www.ciscopress.com/articles/article.asp?p=101629&seqNum=4). ciscopress.com. Cisco Press*. Retrieved 2015-02-05*.

* 1.  [*"Multi-Layer Switching"*](https://web.archive.org/web/20140401064954/http:/www.cisco.com/c/en/us/tech/lan-switching/multi-layer-switching-mls/index.html). Cisco Systems. Archived from [*the original*](http://www.cisco.com/en/US/tech/tk389/tk815/tk850/tsd_technology_support_sub-protocol_home.html) on April 1, 2014*. Retrieved 2011-02-11*.

## External links

* [IETF MPLS Group](http://datatracker.ietf.org/wg/mpls/charter/)
* [What is the difference between a Layer-3 switch and a router?](http://www.dslreports.com/faq/8347)
* [Multilayer Switching](https://www.techrepublic.com/article/multilayer-switching-switching-at-the-speed-of-wire/5033818)

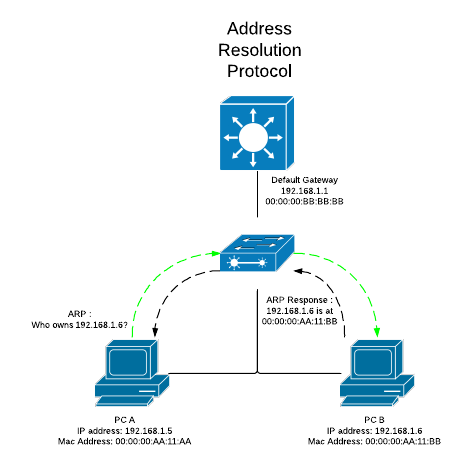
# Layer 3 vs Layer 2 Switching

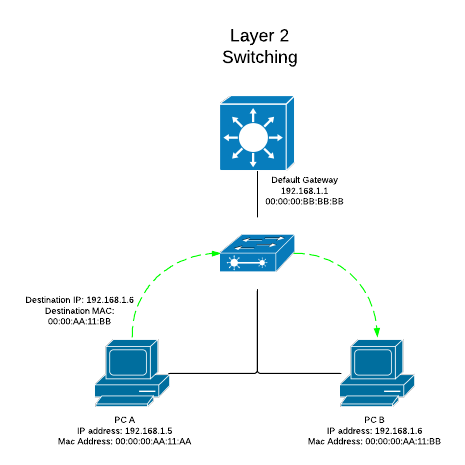
##### Table of contents

1. [Overview](https://documentation.meraki.com/MS/Layer_3_Switching/Layer_3_vs_Layer_2_Switching#Overview)
2. [Additional Resources](https://documentation.meraki.com/MS/Layer_3_Switching/Layer_3_vs_Layer_2_Switching#Additional_Resources)

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

## Overview

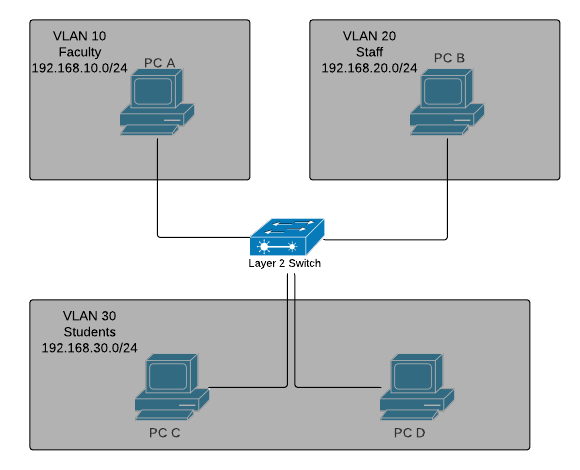
Traditional switching operates at layer 2 of the OSI model, where packets are sent to a specific switch port based on destination MAC addresses. Routing operates at layer 3, where packets are sent to a specific next-hop IP address, based on destination IP address. Devices in the same layer 2 segment do not need routing to reach local peers. What is needed however is the destination MAC address which can be resolved through the Address Resolution Protocol (ARP) as illustrated below:  
****

Here, PC A wants to send traffic to PC B at IP address 192.168.1.6.  It does not know the unique MAC address however, until it discovers it through an ARP, which is broadcasted throughout the layer 2 segment:  
****

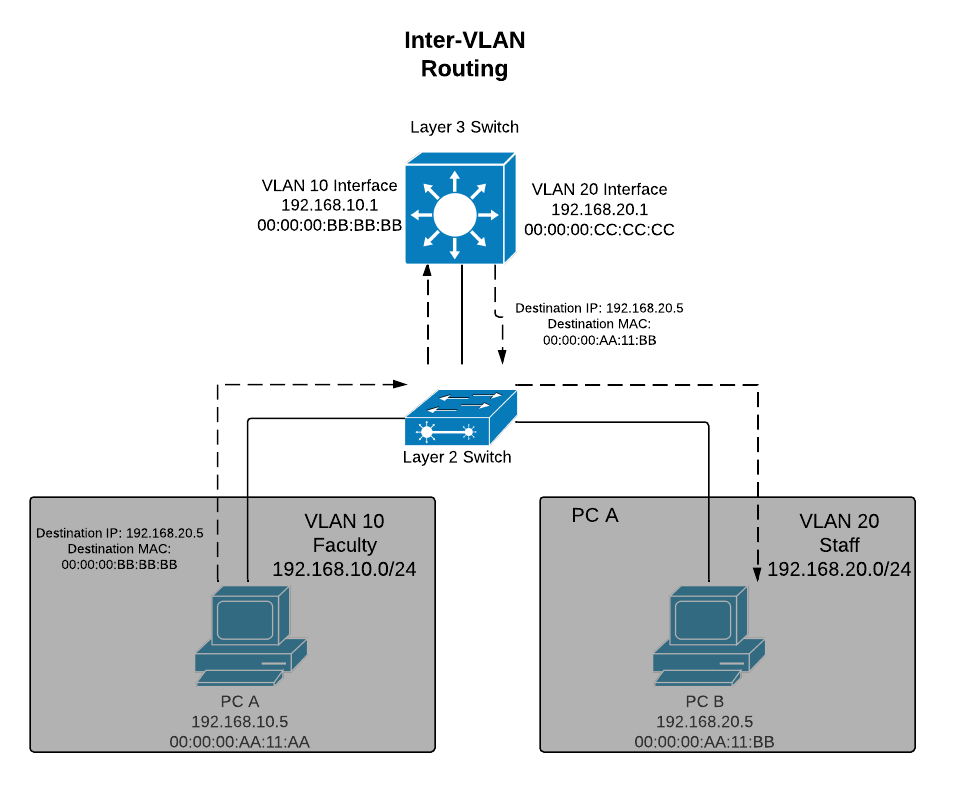
It then sends the packet to the appropriate destination MAC address which the switch will then forward out the correct port based on its MAC-Address-Table.

Within a layer 2 switch environment exists a broadcast domain.  Any broadcast traffic on a switch will be forwarded out all ports with the exception of 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 certain unintended problems, such as broadcast storms, which have the ability to cause network outages.  Also, it may be preferable to separate certain clients into different broadcast domains for security and policy reasons.  This is when it becomes useful to configure VLANs.  A layer 2 switch can assign VLANs to specific switch ports, which in turn are in different layer 3 subnets, and therefore in 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 will be that of the default gateway, which will then accept the packet at layer 2, and proceed to route the traffic to the appropriate destination based on its routing table.

The diagram below shows an example of a layer 3 switching 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:  


## Additional Resources

[Layer 3 switch overview](https://documentation.meraki.com/MS/Layer_3_Switching/MS_Layer_3_Switching_and_Routing) - An overview of how to configure layer 3 routing on Cisco Meraki switches

[Layer 3 switch example](https://documentation.meraki.com/MS/Layer_3_Switching/Layer_3_Switch_Example) - A configuration example using layer 3 routing on Cisco Meraki switches

[Best practices for 802.1q VLAN tagging](https://documentation.meraki.com/zGeneral_Administration/Tools_and_Troubleshooting/Fundamentals_of_802.1Q_VLAN_Tagging) - Information regarding the appropriate use of VLAN tags