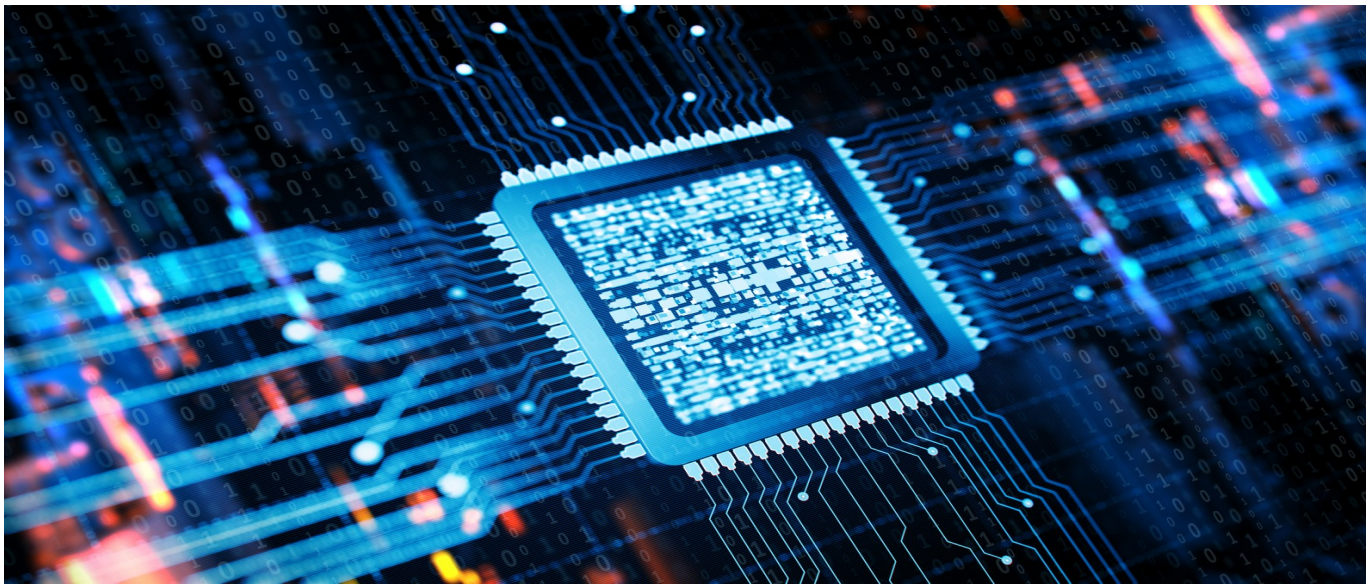
Layer 2 Switching
Technology Brief



In the past a hub was used to connect hosts in a network. A hub is a simple device. It has no knowledge on where to send information to and it always broadcasts all network data over every port. This causes a lot of unnecessary network traffic and consumes unnecessary bandwidth on ports that are not interested in the data. And because of the broadcast behavior, it evidently causes security issues.

A switch is more intelligent than a hub and solves this problem by examining the incoming traffic and by making efficient forwarding decisions for the traffic accordingly. Switches have become an integral part of today's LAN infrastructure.

This article explains layer 2 switching in AimOS.

L2 Switching in AimOS

The AimOS Ethernet solution is targeted and customized for Ethernet switches for various switch ASIC SDKs such as Broadcom® , Marvell® and other switch ASIC suppliers. It supports all the relevant standards and is suited for the most demanding mission critical applications.

Most common L2 features

- Virtual Networking
- Redundancy
- Aggregation
- Differentiated Services

An Ethernet switch operates on the data link layer of the OSI model (layer 2).

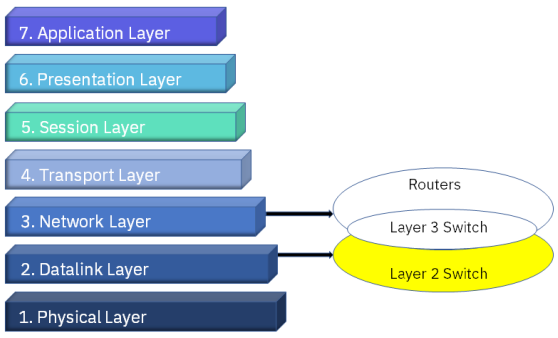


Figure 1: OSI-model

The switch learns the MAC addresses by examining the source MAC address of each received frame on a port and stores it in the forwarding table. This is done in hardware and is therefore, very fast.

Layer 2 Switching
Technology Brief

When a switch receives a frame it uses the destination MAC address of the frame and compares it with entries in the forwarding table. If the MAC address is found in the table, the frame is sent out on the port that was recorded in the matching forwarding table entry. In case no match was found in the forwarding table, the frame is flooded on all ports except on the port it originated from.
It is also possible to configure static unicast or multicast forwarding entries on the switch.

Automatic hardware-based address learning can lead to traffic storms and a non-usable network when a user creates a network loop by accident, e.g. connecting 2 switch ports together. A way to prevent this, is to use a protocol that configures loop free topologies. Examples of such protocols are RSTP, ERPS, MRP, or HSR. These protocols will block all ports on the switch that would otherwise cause a loop.

A VLAN (Virtual Local Area Network) virtually separates LANs. This can be seen as a separate network and it means that when a frame is broadcast, it will only be sent to ports which are in that particular VLAN. Without a VLAN a broadcast frame that is sent by a host will reach all devices on the network. If you need to reach a host in a different VLAN, then a router or router functionality, like a L3 switch is needed. AimOS-E supports a L3-switch. More information on AimValley's expertise on Layer 3 switching.

In order to increase the capacity of a link between two sites, multiple ports can be aggregated (bundled) together to a virtual link using the LAG (Link Aggregation Group). Besides increasing the bandwidth of a link, LAG also adds protection to the link: in case one port connection fails, despite the fact that the link capacity degrades due to one missing link, the other ports remain operational and keep the link intact.

Quality of Service (QoS)

The goal of QoS is to identify different streams or data transfers and to forward each flow according to different priorities. When the bandwidth limits of the network are reached QoS can ensure that specific data streams are prioritized above others. This occurs at the cost of dropping frames with lower priority.

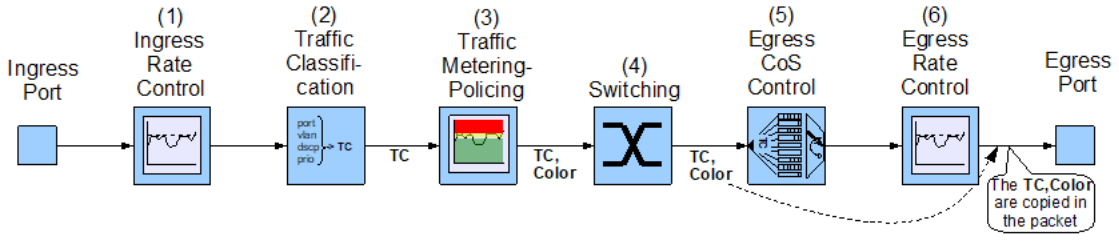


Figure2: Quality of Service (QoS)

AimValley
Utrechtseweg 38
1213 TV Hilversum
The Netherlands
phone +31 35 689 1900
sales@aimvalley.com
www.aimvalley.com

Layer 2 Switching
Technology Brief

Internet Group Management Protocol (IGMP)

For live streams of video images which are watched by many users at the same time, multicast traffic can be used. Typically IGMP (IPv4) or MLD (IPv6) protocols are used to distribute this traffic to end users. Normally layer 2 switches will flood multicast traffic to all ports that are part of the VLAN, which is not always an efficient and desired scenario.

In order to overcome this problem IGMP/MLD snooping can be used. This mechanism snoops IGMP/MLD the Query and Report messages that are transferred between the multicast router and the hosts and configures the layer 2 switch such that it forwards the multicast traffic only to the ports of the hosts that are interested in the stream.

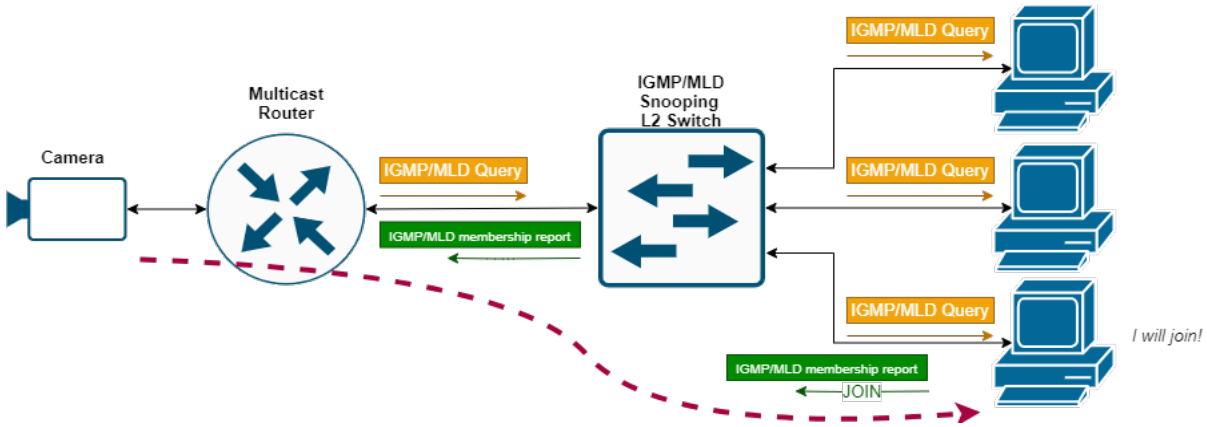


Figure 3: IGMP/MLD snooping

AimValley Expertise

Started in 2003, we have delivered over 100,000 deployed systems with customized and varied flavors of AimOS family to different category of customers:

- Industrial applications
- Telecom applications
- Aerospace applications
- Automotive applications

Visit our website for an extensive overview of our AimOS experience.

Why AimValley?

AimValley is a reliable provider of packet switching technology since 2003, delivering solutions for:

- High speed data processing applications
- Complex FPGA-based accelerated systems
- High speed, low power hardware equipment
- Robust embedded software
- Early adopter of Acceleration Technology

AimValley understands the full complexities as well as the subtle nuances of designing great edge solutions. We excel in building complex systems that are part of your product in the fields of Industry 4.0, Big Data, Healthcare and Transportation markets.

Our combined skills represent all the important aspects required for the development of end-to-end systems.

Our customers enjoy the benefits of working with a strong team with more than 2 000 years engineering experience. AimValley is a trusted partner of Tier 1 customers in Telecom and Industrial markets and has shipped more than 100 000 products.

Quality Focus

- Outstanding track record of on-time delivery
- Best in Class Designs – Time, Budget & Quality
- ISO9001, ISO140001, Ecovadis Platinum CSR