Understanding the Architecture of a Layer-2 Ethernet Switch for Technical Assessment Regarding Cybersecurity

2022-10-17

Preface

The goal of an organization is to protect their assets, maintain privacy, and maintain the trust of customers and stakeholders. To reach this goal the organization is pursuing objectives of safeguard service availability and sensitive information, prevent data from unauthorized access and mitigate potential risks.

Cybersecurity is not a feature of a single hardware component alone. It is a holistic approach that encompasses various aspects of technology, processes, and people.

As an example, The Cybersecurity Framework (CSF) developed by National Institute of Standards and Technology (NIST) provides guidelines and best practices for assessment, implementing and risk management to protect systems from cyber threads (https://www.nist.gov/cyberframework). The framework describes cybersecurity as a comprehensive and ongoing effort and helps to understand the full scope.

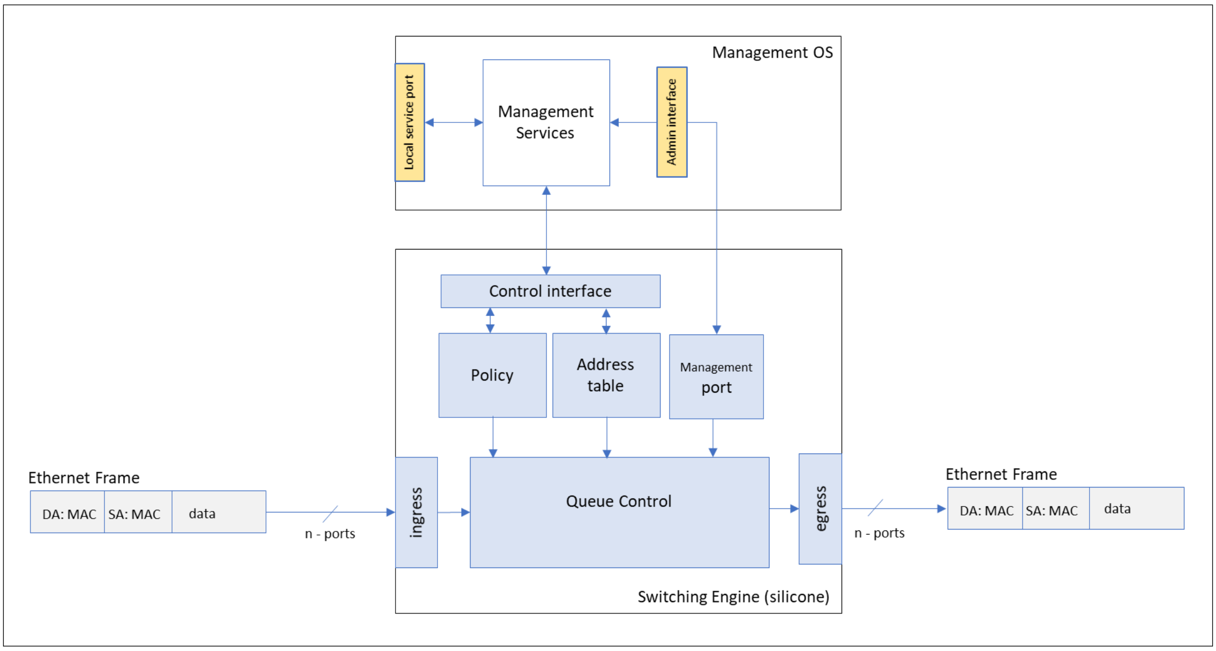
Thus, to guard system, feature details must be well known on a component level. A technical evaluation of used components should be performed to understand to what extent a component represents a vulnerability for the specific attack or how the features of a component can contribute to the system protection.

This article describes the basic architecture of an Ethernet switch to provide technical details for a technical assessment regarding cybersecurity aspects. In this document, an Ethernet switch is defined as a Layer-2 managed standalone device that ensures communication in a local area network (LAN).

Ethernet Switch Architecture

An Ethernet switch is a node in a local area network (LAN). Its primary function is to connect participants to a network at the physical level (Layer-1) and to allow each participant to be addressed at the logical level (Layer-2).
The core component inside the Ethernet Switch is the switching engine, which is responsible for forwarding network traffic. It contains the queue control unit as well as incoming (ingress) and outgoing (egress) buffers. The actual processing of the data transfer takes place fully in the hardware. This guarantees a very low latency (µs range) for the data transmission.

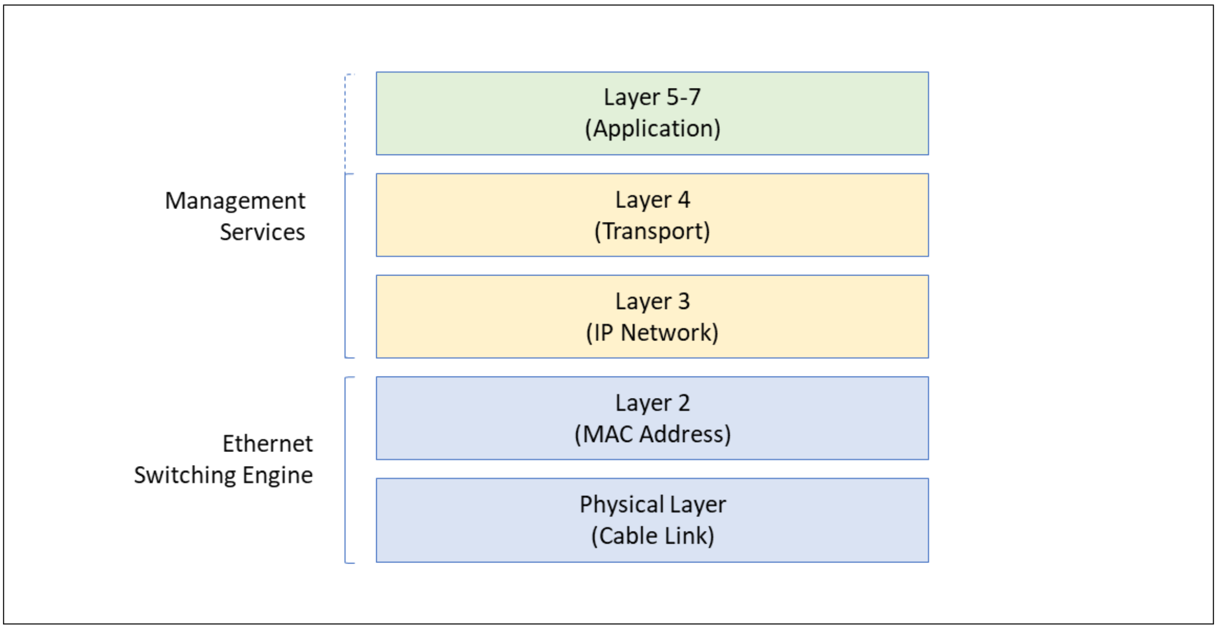
In Layer-2 the addressing is based on MAC addresses. Each network interface has a worldwide unique MAC address. Communication is processed in data packets (frames). Each data packet contains a destination MAC address (DA) and a source MAC address (SA). Based on DA, the queue control unit decides to what port the incoming data packet will be forwarded to. The addresses are stored in a MAC table for this purpose. The MAC table is updated automatically by the queue control unit saving the assignment between port and sender MAC address.



A managed Ethernet switch offers settings to control incoming or outgoing buffers. The settings can also apply filters used for conditional forwarding or further processing of the packets. This enables the support of VLAN and spanning tree (STP/RSTP) or DHCP options.
The settings are applied through a control interface. This is usually the interface for management. The settings are commonly referred as configuration of the switch. The management services are software programs that run in an embedded operating system (management OS).

A managed Ethernet switch offers at least two interfaces for administration: A local service port often designed as a USB or serial port. And a network interface that allows access to management services over the network (admin interface). This interface behaves like a usual network participant and can be addressed via IP in the network. A special port is provided in the switching engine for this purpose, the internal management port.

The management port can handle both regularly and management frames. The management frames are tagged as such and are always routed from queue control to the management port. The frames are then available for service (e.g. DHCP) to be processed. These services usually belong to Layer-4 and higher. Whoever has access to the management services has control over the device.



Packet Inspection in Layer-2 Ethernet Switch

A Layer-2 Ethernet switch transmits data without analyzing its content (payload). The physical transport of frames takes place exclusively in the hardware (silicone). All other services and protocols are performed in the OS as part of the management software (Management Services).

To provide network management and support network protocols the Ethernet frames are forwarded to the management software. The software then can process the frames or data accordingly. Theoretically, all frames can be processed through software instead of the switching engine. The software could then analyze and filter the packets according to a specific policy, like a firewall. For a Layer-2 device this is not a practical approach.

The management software runs on an embedded CPU. The computing power of a usual embedded system will not be sufficient to forward the frames smoothly while performing packet inspection and applying filtering rules. Thus, a software-based packet inspection will lead to a strong performance loss. The throughput of the data transmission is drastically reduced as soon as the management software intervenes in the packet processing. This applies to any firewall and encryption mechanisms done by software on the Ethernet frame level.

Software Updates

Software update refers to the process of update the operation system (Management OS). This process typically includes the exchange of the OS on the embedded device. Updates of the silicon functions are technically not supported in this context.

Conclusion

It is crucial to acknowledge that cybersecurity is an ongoing process, requiring continuous monitoring, updates, and adherence to best practices.
To define, implement and maintain sufficient security measures it is crucial to understand the technology in its core, on the component level.

This paper described the architecture of the Ethernet switch and provided valuable insights into its technology with a specific focus on cybersecurity. This helps system engineers to understand the technology and function, enabling them to assess cybersecurity aspects.

A Layer-2 Ethernet switch forwards data traffic through a silicone switching engine, while management software handles network protocols and services.

Software-based packet inspection can significantly reduce performance and throughput and therefore is not of practical use to filter traffic by the management OS.

Ethernet switches support software updates of the management OS.