Introduction to Matter

Introduction to Matter

Introduction to Matter

Why Matter?

The Connectivity Standards Alliance seeks to enable smart home devices to be secure, reliable, and interoperable with other Internet of Things (IoT) devices, regardless of manufacturer. One of the biggest pain points of smart home devices is the various application-layer implementations that limit the compatibility of different smart home devices. Therefore, Matter was adopted so that matter-enabled devices, under the same standard, provide a better experience for both manufacturers and users.

While Matter was created to make the IoT seamless and effortless for users, it is important to acknowledge the complexity involved under the surface. Matter leverages a range of tools to enable seamless and secure connectivity within an IoT system. Understanding these tools is crucial for a comprehensive overview of this technology.

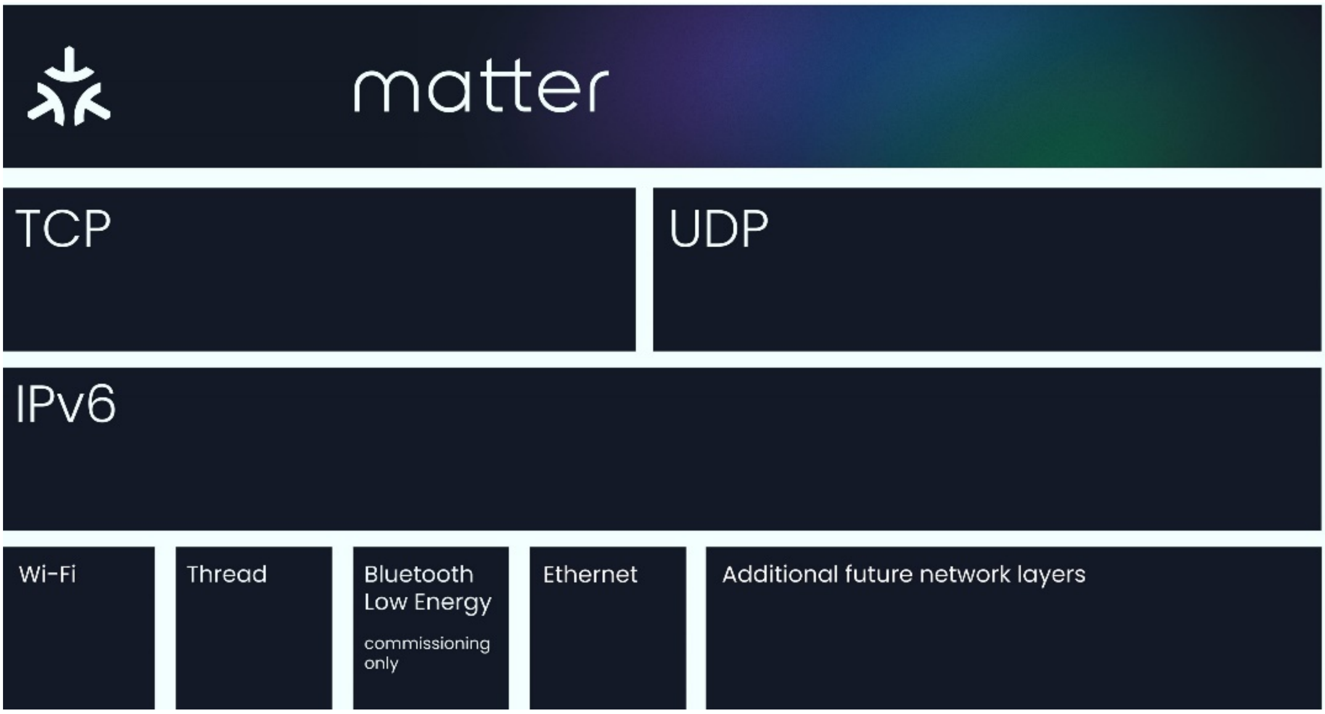
Matter Enablement

Matter implements the Application Layer of the Open Systems Interconnection (OSI) model. It builds on the lower layers, such as the transport and network layers, to enable reliable communication between nodes.

Matter may sit on top of two prominent connectivity technologies: Thread and Wi-Fi. Thread is a low-power wireless mesh networking protocol that facilitates reliable communication between nodes. It enables extended coverage and reliable connections to improve the overall performance of IoT ecosystems.

Matter is an IPv6-based protocol that utilizes transport layer protocols like TCP/UDP to facilitate network addressing and reliable transmission of data packets, respectively. Due to this, Matter is compatible with multiple connectivity options (such as Thread and Wi-Fi). This flexibility allows Matter-enabled devices to communicate over various network protocols, ensuring broad compatibility and integration with different networking technologies.

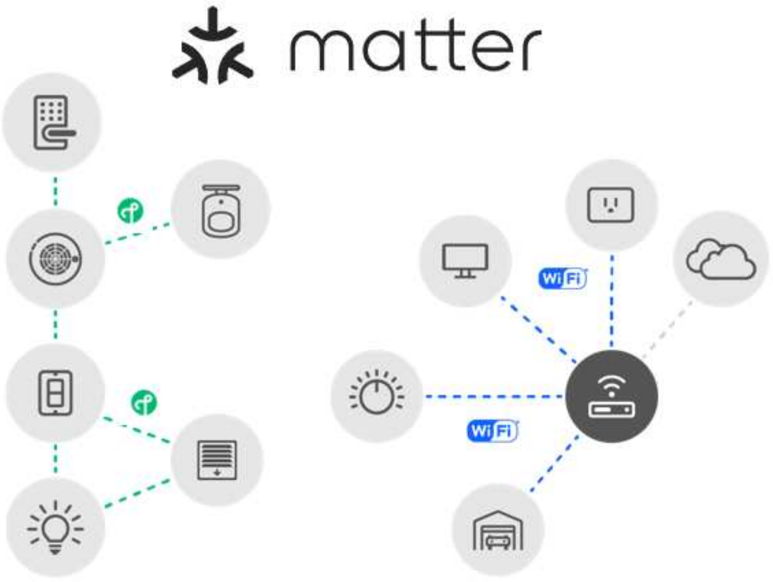
The true power of Matter lies in its commitment to interoperability. Industry leaders such as Google, Apple, Amazon, and Samsung Smart Things have implemented Matter in their IoT devices, fostering wider adoption from other manufacturers. Matter also supports bridging from other existing technologies, such as Zigbee, Bluetooth® Mesh, and Z-Wave. This allows already existing IoT technology to be integrated into an interoperable environment. The compatibility and seamless integration across brands create a unified ecosystem where your smart devices work harmoniously.



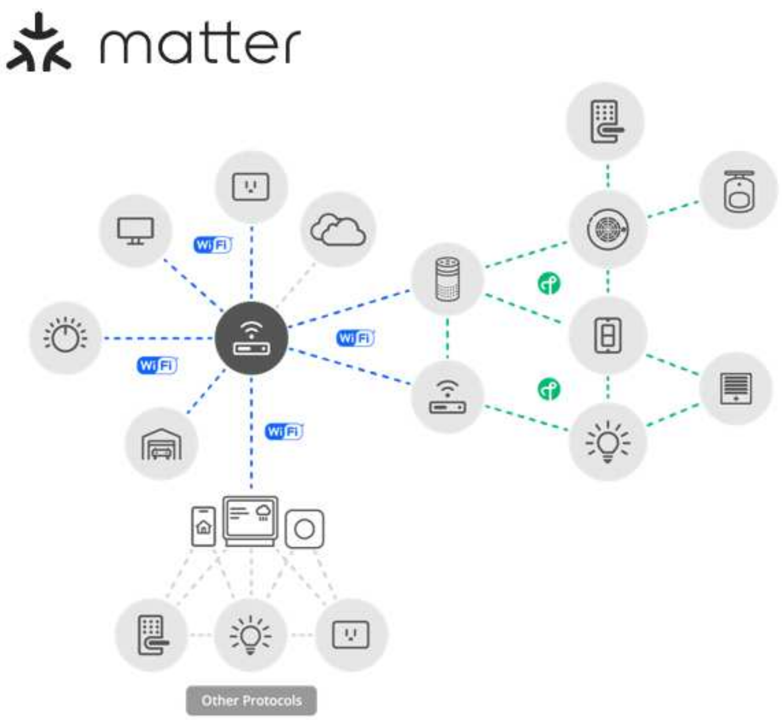
Matter Network Architecture

In theory, Matter can sit on top of any IPv6-bearing network. However in practice, the Matter specifications solely focus on three link layer technologies, enabling Matter to run on Ethernet, Wi-Fi, and Thread 802.15.4 networks. As mentioned above, one of the great benefits of Matter is its flexibility, especially when it comes to network configuration. The Matter protocol can operate without a globally-routable IPv6 infrastructure and allows the flexibility of having multiple Matter networks run over the same set of constituent IP Networks.

Two common underlying network topologies are commonly used in Matter. The first is known as a Single Network topology, where Matter runs solely over one Network. This means the Matter Network could run over one 802.15.4 Thread network or over a Wi-Fi network. In this scenario, all Matter devices are connected to the same single logical network.



The other, more common, network topology is the star network, which consists of multiple peripheral networks joined together by a central hub network. If a peripheral network is used, it must be directly joined to a hub via one or more border routers. A border router (or an edge router) is a special router that can provide routing services between two IP Subnets, effectively acting as a bridge between the two different networks. This enables a lot of flexibility and interoperability between various home networks that can all be interconnected.



Regardless of the network topology being used, Matter has a concept of Fabrics. A Matter Fabric is a security domain that contains a collection of nodes. These nodes can be identified and can communicate with each other within the context of that security domain. Each Matter Fabric has a unique Node ID for each node within the fabric and has a unique Fabric ID. Any Matter device can be a part of multiple Matter fabrics, and in turn will have multiple associated Node IDs / Fabric IDs depending on the fabric it is communicating with.

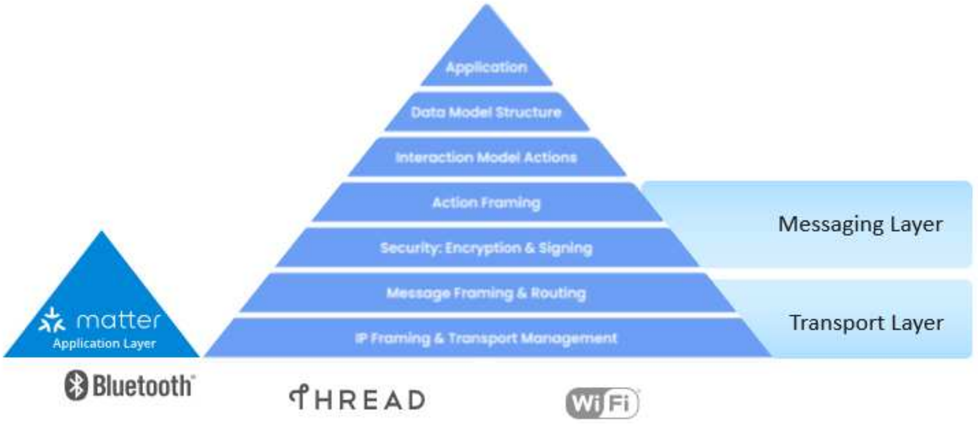
Below is a table of some basic Identifiers that are commonly used in Matter to identify and communicate with nodes on the fabric.

Identifiers	Definition
Fabric	64 bit number that uniquely identifies the Matter fabric.
Vendor	16 bit number that uniquely identifies a particular product manufacturer, vendor, or group thereof.
Product	16 bit number that uniquely identifies the product from a specific vendor.
Group	16 bit number ID set of nodes across a Matter Fabric
Universal Group	16 bit subrange of the Group ID reserved for groups across Matter Standard. Specifically a UID for all nodes, all non-ICD nodes, and all proxies.
Operational Node	64 bit number that uniquely identifies an individual node on the fabric
PAKE Key Identifiers	This is a subrange of Node ID used to assign an Access Control subject to a particular PAKE key. This creates an ACL (Access Control List) entry to provide admin access via a PASE session.

Matter Layered Architecture

Matter is split up into a layered architecture to help separate the different responsibilities and encapsulate various pieces of the protocol stack. The following diagram shows the various interactions between the Matter application stack layers as defined by the

Matter specification. For implementation purposes, the last four layers are handled as a Messaging Layer and a Transport layer.



- The Application Layer of the Matter stack is the highest layer, and corresponds to the high-level logic of the device. The user application is built on the unified data model, which helps improve interoperability.
- The Data Model layer corresponds to how the data and action elements support the functionality of the application, such as the defines of the elements, namespaces for endpoints, clusters, and attributes in the application.
- The Interaction Model handles, as the name suggests, the interactions between the nodes and is responsible for how data is transferred between nodes. Both the Data Model and Interaction Model are inherited from the well-known dotdot standard used by Zigbee.
- The Action Framing layer is where the interactions are transformed into a message payload.
- The Security Layer takes the payload and encrypts and appends the packet with a MAC (Message authentication code).
- From the security layer, the packet transfers down to the Transport layer to what the Connectivity Standards Alliance refers to as the Message Framing and Routing layer. This updates the payload with the necessary routing information such as fabric and Node ID.
- Finally the packet is sent to the Transport and IP Framing layer, from which the payload is sent through the IP network either through TCP (which is not yet currently supported) or Matter's Message Reliability Protocol, a software layer on top of UDP, for IP management of the data. Note that the IP Framing in Matter is handled by the Networking Protocol stack to handle this.

Once the data is received on a peer device, it travels up the Matter Protocol stack in reverse and delivers the message to the Application layer.

Matter Security

As mentioned before, one of the main benefits of using Matter is the enhanced security that it offers. Matter offers security at many layers throughout the network. Many security features are integrated into commissioning a Matter device onto an existing network. Matter requires all devices to have a device-specific passcode that delivers "proof of ownership" to commissioning devices and requires all devices to have immutable credentials that can be cryptographically verified to indicate that the joining devices are Matter-certified devices. In fact, the network credentials are only given to the Matter device after the device has been authenticated and verified. This helps keep the Matter network secure from foreign and unsecure devices, significantly improving the overall network security. Furthermore, Matter enables encryption and authentication to all unicast messages, as well as providing relay protection. Below is a list of commonly-used Matter security terms.

Concepts	Definition
DAC (Device Attestation Certificate)	This is an immutable certificate of credentials that can be cryptographically verified to confirm that the device is a certified Matter device.
PASE (Passcode Authentication Session Establishment)	This process at the Commissioning stage uses a passcode provided out-of-band (like a device's QR code) to commission a Matter device on the network.
CASE (Certificate Authentication Session Establishment)	This process at the Operational stage establishes and provides an authentication key exchanged between two devices.

More detailed information on Matter security can be found in Matter Security and Matter Commissioning.