**Internet Protocol Authentication Header**

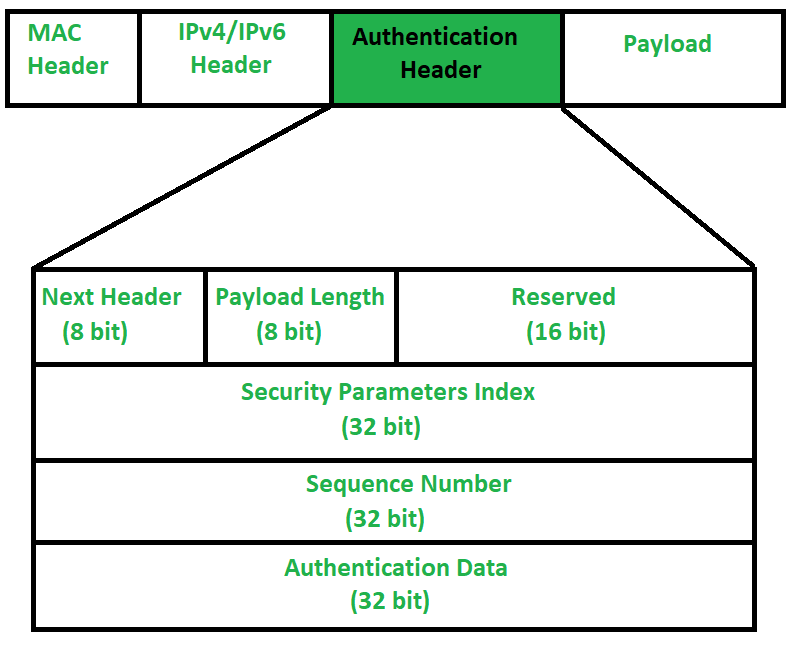
* The Internet Protocol Authentication Header (AH) is a component of the IPsec (Internet Protocol Security) suite that provides data integrity, data origin authentication, and optional anti-replay protection for IP packets.
* Authentication Header ensures that the data was not modified during transmission and verifies the identity of the sender

**What is an Authentication Header?**

* The Authentication Header (AH) is a security protocol used within the IPsec suite.
* Its primary function is to ensure that the message remains unmodified during transmission from the source to destination.
* It adds a header to IP packets, containing a checksum and a [digital signature](https://www.geeksforgeeks.org/digital-signatures-certificates/). Its main functions are:

1. **Message Integrity:** Verifies that the data **has not been altered** during transmission.
2. **Source Authentication:** Confirms that the **data originates from the expected source**.

**Authentication Header Format:**



1. **Next Header (8-bit):** Identifies the type of header that comes after the Authentication Header (e.g., IPv4, IPv6, TCP, UDP).
2. **Payload Length:** Indicates the size of the Authentication Header, calculated using a scaling factor.
3. **Reserved (16-bit):** A field set to **zero** by the sender, reserved for future use.
4. **Security Parameter Index (SPI) (32-bit):** It is used to give a unique number to the connection built between the Client and Server.
5. **Sequence Number (32-bit):** Unique Sequence numbers are allotted to every packet so that on the receiver side packets can be arranged properly. The sequence number starts from 0 and goes up to **2^32 - 1**. If the counter runs out, the connection is re-established.
6. **Authentication Data (Variable Length):** Contains the **Integrity Check Value (ICV)**, which ensures that the data hasn’t been tampered with. It’s generated using a **hashing algorithm** and **secret key**.

**Authentication Header Works:**

When a packet is sent from **Source A to Destination B**, it contains **data** and a **header**. The **Authentication Header (AH)** performs two key tasks:

1. **Verifies the Source:** It ensures that the data **comes from the expected sender** (Source A).
2. **Checks for Modifications:** It checks if the **data has been altered** during transmission to ensure integrity.

However, some parts of the **IP header** (like **hop count, options, and extension headers**) can change during transmission and **are not protected by the Authentication Header**. The Authentication Header focuses only on securing the **essential fields** that need protection, ensuring the core data remains intact and unmodified.

**Modes of Operation in Authentication Header (AH):**

1. **Transport Mode:**
   * The **Authentication Header** is placed between the **IP header** and the **TCP header**, protecting only the **data** (not the IP header). It’s used for **device-to-device communication**.
2. **Tunnel Mode:**
   * The **entire original packet** is authenticated, with a **new outer IP header** added. It’s used for **network-to-network communication** (e.g., VPNs).