IDS   
is designed to only provide an alert about a potential incident, which enables a security operations center (SOC) analyst to investigate the event and determine whether it requires further action.

IPS  
on the other hand, takes action itself to block the attempted intrusion or otherwise remediate the incident.

Intrusion Detection System: An IDS is designed to detect a potential incident, generate an alert, and do nothing to prevent the incident from occurring. While this may seem inferior to an IPS, it may be a good solution for systems with high availability requirements, such as industrial control systems (ICS) and other critical infrastructure. For these systems, the most important thing is that the systems continue running, and blocking suspicious (and potentially malicious) traffic may impact their operations. Notifying a human operator of the issue enables them to evaluate the situation and make an informed decision on how to respond.

Intrusion Prevention System: An IPS, on the other hand, is designed to take action to block anything that it believes to be a threat to the protected system. As malware attacks become faster and more sophisticated, this is a useful capability because it limits the potential damage than an attack can cause. An IPS is ideal for environments where any intrusion could cause significant damage, such as databases containing sensitive d.

IDSs and IPSs both have their advantages and disadvantages. When selecting a system for a potential use case, it is important to consider the tradeoffs between system availability and usability and the need for protection. An IDS leaves a window for an attacker to cause damage to a target system, while a false positive detection by an IPS can negatively impact system usability.

An internal router operates at the network layer (Layer 3) of the OSI model and is crucial for efficient communication within a local network. It uses routing tables to make decisions about how to forward data packets between devices. These routers play a key role in connecting different segments of a network and ensuring that data reaches its intended destination.

Internal routers are commonly used in homes, businesses, and larger organizations to manage the flow of information among computers, servers, and other networked devices. They facilitate communication within the internal network and often provide features such as DHCP (Dynamic Host Configuration Protocol) for automatic IP address assignment and NAT (Network Address Translation) for sharing a single public IP address among multiple devices.

In contrast to external routers that connect different networks, internal routers focus on directing traffic within a single network, enhancing its overall efficiency and security.

Routers   
operate by forwarding data packets between different networks, determining the optimal path for each packet based on the destination IP address. Here's a basic overview of how routers work:

1. \*Packet Forwarding:\* When a device on one network wants to communicate with a device on another network, it sends out a data packet. Routers examine the destination IP address of each packet and use routing tables to determine where to send it next.

2. \*Routing Tables:\* Routers maintain routing tables, which are essentially maps of the network. These tables contain information about how to reach different IP addresses or network segments. The router consults these tables to decide the next hop for a packet.

3. \*IP Addressing:\* Routers play a crucial role in IP addressing. They assign unique IP addresses to devices on the local network using protocols like DHCP. This enables devices to communicate within the network and also helps in the routing process.

\*DHCP (Dynamic Host Configuration Protocol):\* DHCP is a network protocol used by routers to dynamically allocate IP addresses to devices on the network. When a device connects to the network, it requests an IP address from the router, which then assigns an available IP address to that device.

4. \*Network Address Translation (NAT):\* Routers often use NAT to manage the use of public IP addresses. When devices on the local network communicate with the internet, the router translates their private IP addresses into a single public IP address. This allows multiple devices to share a single public IP address.

In summary, routers enable communication between different networks by forwarding data packets based on destination IP addresses. They also manage IP addressing within a local network, assigning unique addresses to devices through DHCP and using NAT to facilitate internet communication.

DORA stands for "Discover, Offer, Request, Acknowledge," and it refers to the four steps involved in the Dynamic Host Configuration Protocol (DHCP) process. DHCP is a network protocol that allows a device to obtain an IP address dynamically from a DHCP server. Here's a brief overview of each step in the DORA process:

1. \*Discover:\* When a device (such as a computer or smartphone) connects to a network and needs an IP address, it sends a DHCP Discover message to discover available DHCP servers on the network. This broadcast message essentially asks, "Is there a DHCP server available?"

2. \*Offer:\* DHCP servers that receive the Discover message respond with a DHCP Offer. This Offer includes an IP address that the server is willing to lease to the requesting device. The DHCP Offer is a unicast message sent directly to the device making the request.

3. \*Request:\* Upon receiving one or more DHCP Offers, the requesting device chooses one and sends a DHCP Request. This Request confirms the chosen DHCP server and formally requests the offered IP address. The device may receive multiple Offers but will only Request one.

4. \*Acknowledge:\* The DHCP server, upon receiving the Request, sends a DHCP Acknowledge (ACK) message to the requesting device. This message confirms the IP address lease and provides additional configuration information, such as the subnet mask, default gateway, and DNS servers.

The DORA process ensures a dynamic and automated way of assigning IP addresses to devices on a network, making network management more efficient. DHCP is commonly used in local area networks (LANs) and is especially practical in scenarios where manual IP address configuration would be impractical or cumbersome.

Switches use MAC addresses (Media Access Control addresses) to forward data within a local network efficiently. Here's how switches and MAC addresses work together:

1. \*Learning MAC Addresses:\* Switches learn the MAC addresses of devices connected to their ports. When a device sends a frame (a unit of data at the data link layer), the switch examines the source MAC address in the frame and associates it with the port through which the frame arrived. This process is known as MAC address learning.

2. \*MAC Address Tables:\* Switches maintain MAC address tables (also called forwarding tables or MAC tables) that map MAC addresses to specific switch ports. These tables help the switch make forwarding decisions based on the destination MAC address of incoming frames.

3. \*Forwarding Decision:\* When a frame with a specific destination MAC address arrives at the switch, the switch checks its MAC address table to determine the corresponding port. If the MAC address is in the table, the switch forwards the frame only to the port where the destination device is connected. If the MAC address is not in the table, the switch may flood the frame to all ports (except the source port) to learn the location of the device.

4. \*Reducing Network Traffic:\* Switches significantly reduce network traffic compared to traditional hubs because they selectively forward frames based on MAC addresses. Unlike hubs, which broadcast data to all connected devices, switches make more intelligent forwarding decisions, resulting in more efficient use of network bandwidth.

In summary, switches leverage MAC addresses to efficiently forward data within a local network by learning the association between MAC addresses and specific switch ports. This process improves network performance and reduces unnecessary broadcast traffic.

The physical address -- which is also called a media access control, or MAC, address -- identifies a device to other devices on the same local network.   
  
The internet address -- or IP address -- identifies the device globally. A network packet needs both addresses to get to its destination.

A MAC address is responsible for local identification.

IP address for global identification.

This is the primary difference between a MAC address and IP address, and it affects how they differ in their number of bits, address assignment and interactions. The MAC address is only significant on the LAN to which a device is connected, and it is not used or retained in the data stream once packets leave that network.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a network protocol used to automate the process of configuring devices on IP networks, thus allowing them to use network services such as DNS, NTP, and any communication protocol based on UDP or TCP. A DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks. DHCP is an enhancement of an older protocol called BOOTP.