# SNS COLLEGE OF TECHNOLOGY

**Coimbatore-35**
**An Autonomous Institution**

## Department of Information Technology

**Course Name – 19IT302 Internet of Things**

**III Year / V Semester**

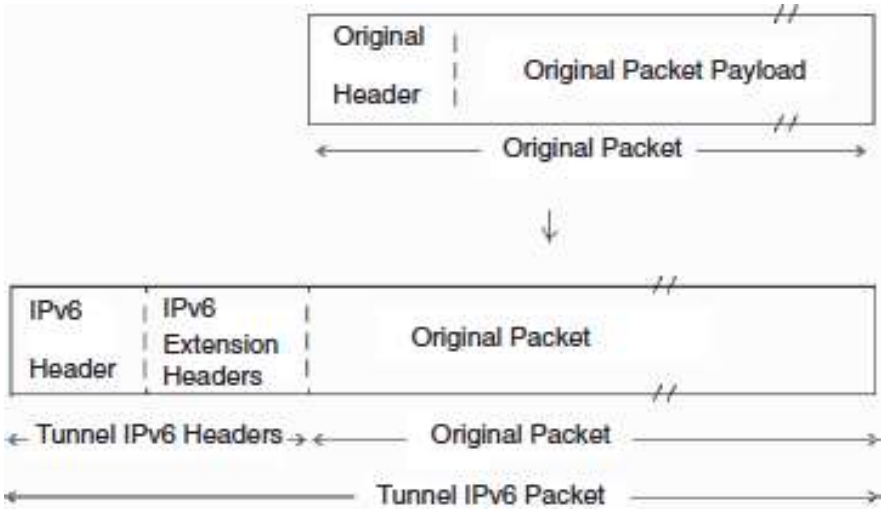
**Unit 4 – IPv6 TECHNOLOGIES FOR THE IOT**

**Topic 2- Motivations – IPv6 Tunneling, IPSec**

# IPv6 - Tunneling

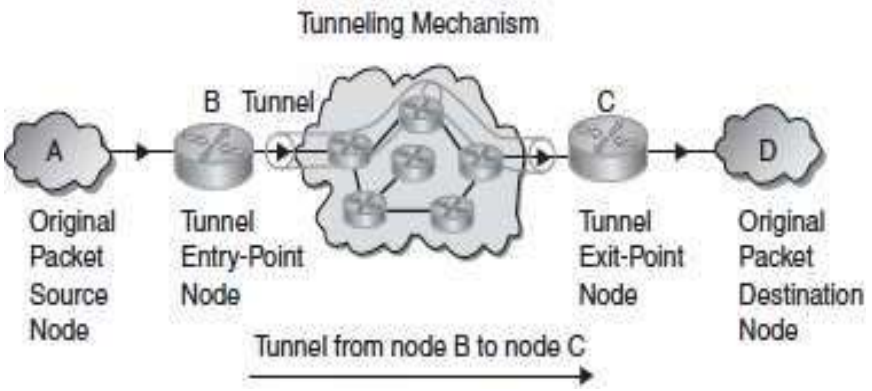
- IPv6 tunneling is a technique for establishing a “virtual link” between two IPv6 nodes for transmitting data packets as payloads of IPv6 packets.

- From the perspective of the two nodes, this “virtual link,” called an IPv6 tunnel , appears as a point-to-point link on which IPv6 acts like a link-layer protocol.



# IPv6 - Tunneling

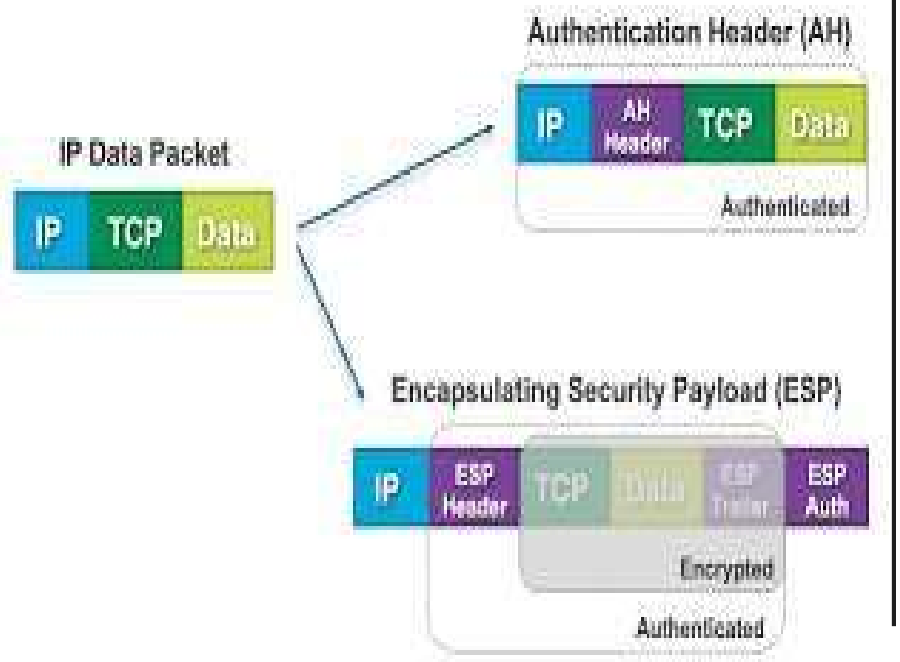
- One node encapsulates original packets received from other nodes or from itself and forwards the resulting tunnel packets through the tunnel.
- The other node decapsulates the received tunnel packets and forwards the resulting original packets toward their destinations, possibly itself.
- The encapsulator node is called the tunnel entry-point node, and it is the source of the tunnel packets.
- The decapsulator node is called the tunnel exit point, and it is the destination of the tunnel packets.



# IPv6 - IPSec

- IPsec provides network-level security where the application data is encapsulated within the IPv6 packet
- IPsec itself is a set of two protocols: ESP and AH.
- IPsec utilizes the AH and/or ESP header to provide security.
- IPsec, with ESP, offers integrity and data origin authentication, confidentiality, and optional (at the discretion of the receiver) antireplay features.
- IPsec with AH offers integrity.

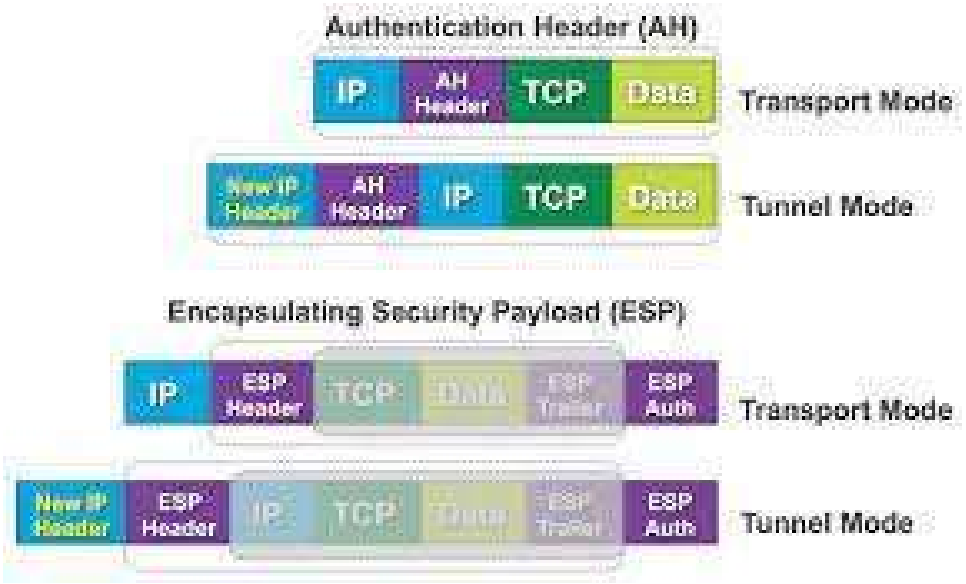
Both the AH and ESP header may be employed as
- Tunnel mode
- Transport mode



# IPv6 - IPSec

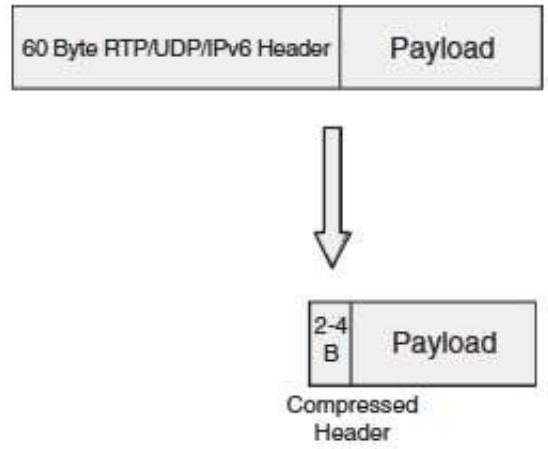
Tunnel mode
The protocol is applied to the entire IP packet. This method is needed to ensure security over the entire packet, where a new IPv6 header and an AH or ESP header are wrapped around the original IP packet.

Transport mode
The protocol is just applied to the transport layer (i.e., TCP, UDP, ICMP) in the form of an IPv6 header and AH or ESP header, followed by the transport protocol data (header, data).



# IPv6 - HEADER COMPRESSION SCHEMES

- The packet header size doubled from 20 bytes in IPv4 to at least 40 bytes in IPv6.
- The use of network-layer encryption mechanism nearly doubles IP operational overhead.
- Currently, Header Compression in wireless and video applications (especially in an IPv6 environment) may well drive future deployment of the technology.
- HC algorithms can reduce the performance and throughput impact of expanded IPv6 packet headers and protocol-imposed overhead.
- Traditionally, compression is applied to layer 3 (IP) and several layer 4 Protocol headers; for example, RTP/UDP/IPv6 headers can be compressed from 60 bytes to 2–4 bytes.



# IPv6 - HEADER COMPRESSION SCHEMES

Two compression protocols emerged from the IETF in recent years:

(i) Internet protocol header compression (IPHC),

A scheme designed for low bit error rate (BER) links. It provides compression of TCP/IP, UDP/IP, RTP/UDP/IP, and ESP/IP header; enhanced compression of RTP/UDP/IP (ECRTP) headers is also used.

(ii) Robust header compression (ROHC)

It is a scheme designed for wireless links that provides greater compression compared to IPHC at the cost of greater implementation complexity. This is more suitable for high BER, long RTT links and supports compression of ESP/IP, UDP/IP, and RTP/UDP/IP header.

# IPv6 - QoS

The IPv6 header has two QoS-related fields:

- 20-bit flow label - IntServ-based environments
- 8-bit traffic class indicator - DiffServ-based environments

- Expedited forwarding (EF): aims at providing QoS for the class by minimizing jitter and is generally focused on providing stricter guarantees;

- Assured forwarding (AF): inserts at most four classes with at most three levels of packets dropping categories.

# THANK YOU