Lecture 3.2

Internet Protocol – IPv6

Dr. Vandana Kushwaha

Department of Computer Science

Institute of Science, BHU, Varanasi

Internet Protocol Version 6(IPv6)

- **IPv4** has some **deficiencies** that make it **unsuitable** for the **fast-growing Internet**.
  - Despite all **short-term solutions**, such as **classless addressing** and **NAT, address depletion** is still a long-term problem in the Internet.
  - The **Internet** must accommodate **real-time audio and video transmission**. This type of transmission requires **minimum delay** strategies and **reservation of resources** not provided in the **IPv4** design.
  - The **Internet** must accommodate **encryption** and **authentication** of **data** for some applications. **No encryption** or **authentication** is provided by **IPv4.**
- To overcome these **deficiencies, IPv6** (Internetworking Protocol, version 6), also known as **IPng** (Internetworking Protocol, next generation), was proposed and is now a standard.

Advantages of IPv6

- **Larger address space**
  - An **IPv6** address is **128 bits** long.
  - Compared with the **32-bit** address of **IPv4,** this is a **huge increase** in the **address space.**
- **Better header format**
  - **IPv6** uses a **new header format** in which **options** are **separated** from the **base header** and **inserted**, **when needed**, between the **base header** and the **upper-layer data.**
  - This **simplifies** and **speeds up** the **routing process** because most of the options do not need to be checked by routers.

Advantages of IPv6

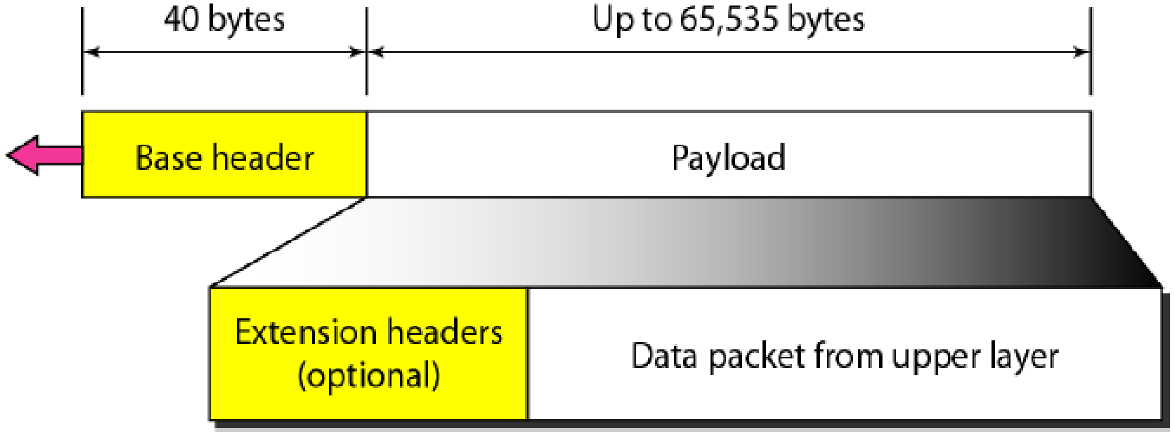
- **Allowance for extension**
  - **IPv6** is designed to allow the **extension** of the **protocol** if required by **new technologies** or applications.
- **Support for resource allocation**
  - In **IPv6,** the **type-of-service** field has been **removed**, but a mechanism (called **flow *label***) has been added to enable the **source** to request **special handling** of the **packet.**
  - This mechanism can be used to **support traffic** such as **real-time audio** and **video**.

Advantages of IPv6

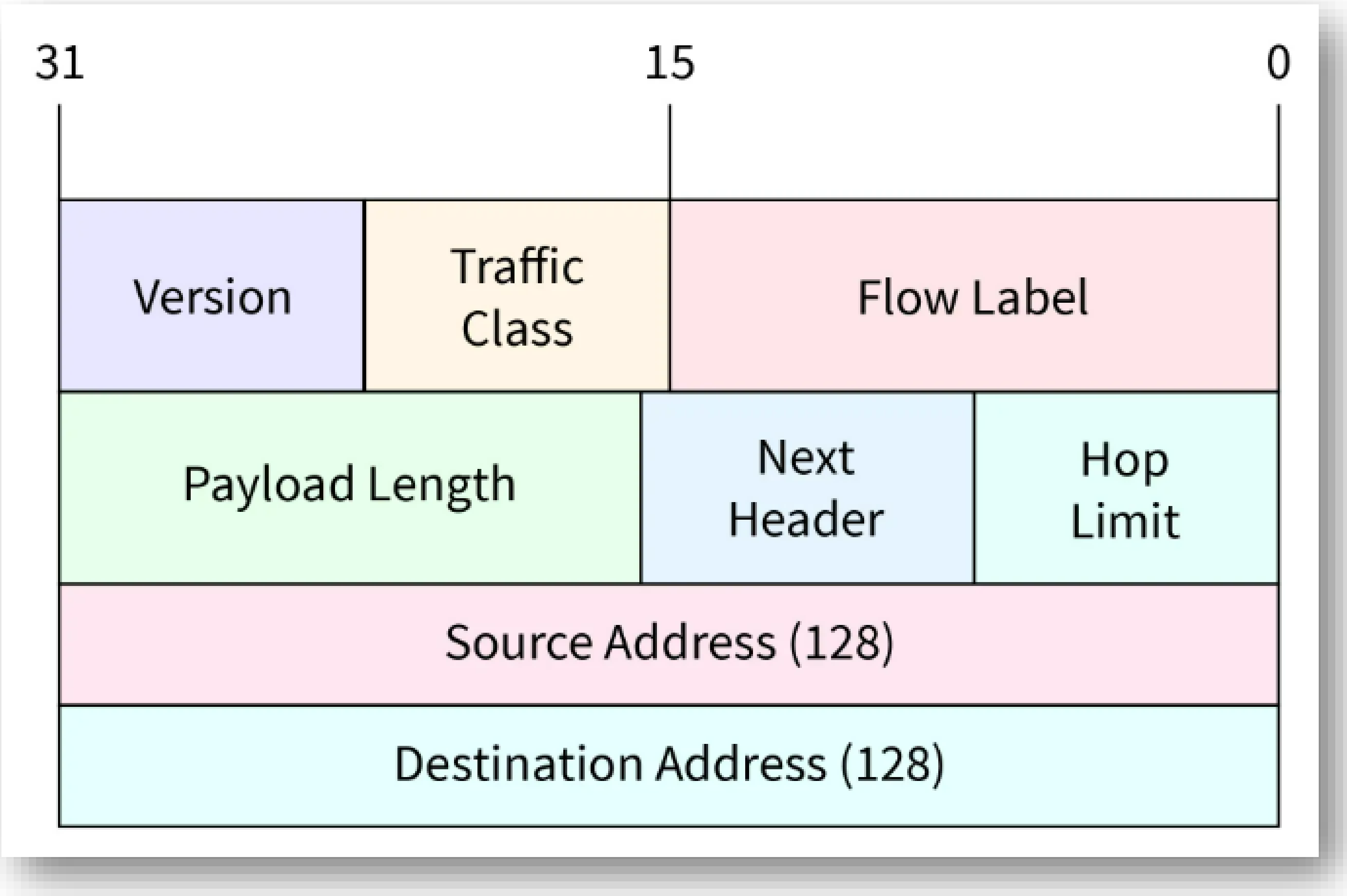
- **Support for more security**
  - The **encryption** and **authentication** options in **IPv6** **provide** **confidentiality** and **integrity** of the **packet.**

IPv6 Packet Format

- Each **IPv6 packet** is composed of a **mandatory base header** followed by the **payload**.
- The **payload** consists of **two parts**:
  - **optional extension headers** and **data** from an **upper layer**.
- The **base header** occupies **40 bytes**, whereas the **extension headers** and **data** from the **upper layer** contain up to **65,535 bytes** of information.



IPv6 Base Header



IPv6 Base Header

Base header has **eight fields.** These fields are as follows:

i. **Version (4 bits)**

- This **4-bit** field defines the **version number** of the **IP.**
- For **IPv6**, the value is **6 (0110)**.

ii. **Priority/Traffic Class (8 bits).**

- The first **6 bits** of the **Traffic Class** field represents the **DSCP field** used for defining the **priority level** of a **datagram.**
- And the last **2 bits** are used for **ECN**(Explicit Congestion Notification).

IPv6 Base Header

iii. Flow label (20 bits)

- The **flow label** is designed to provide **special handling** for a particular **flow** of **data.**
- **Flow Label** field is used by a **source** to **label** the **packets belonging** to the **same flow** in order to request **special handling** by intermediate **IPv6 routers**.
- In order to distinguish the **flow**, an intermediate **router** can use the **source address,** a **destination address**, and **flow label** of the **packets.**
- Between a **source** and **destination**, **multiple flows** may exist because many **processes** might be running at the same time.
- **Routers** or Host that does not support the functionality of **flow label** field and for default router handling, **flow label** field is **set** to **0.**

IPv6 Base Header

iv. Payload length

- The **2-byte** payload length field defines the **length** of the **IP datagram** excluding the **base header.**
- The **payload Length** field includes **extension headers**(if any) and an **upper-layer data.**

v. Next header

- The **next header** is an **8-bit field** defining the **header** that **follows** the **base header** in the datagram.
- **IPv6 packet** may contain **zero, one** or **more extension headers .**

IPv6 Base Header

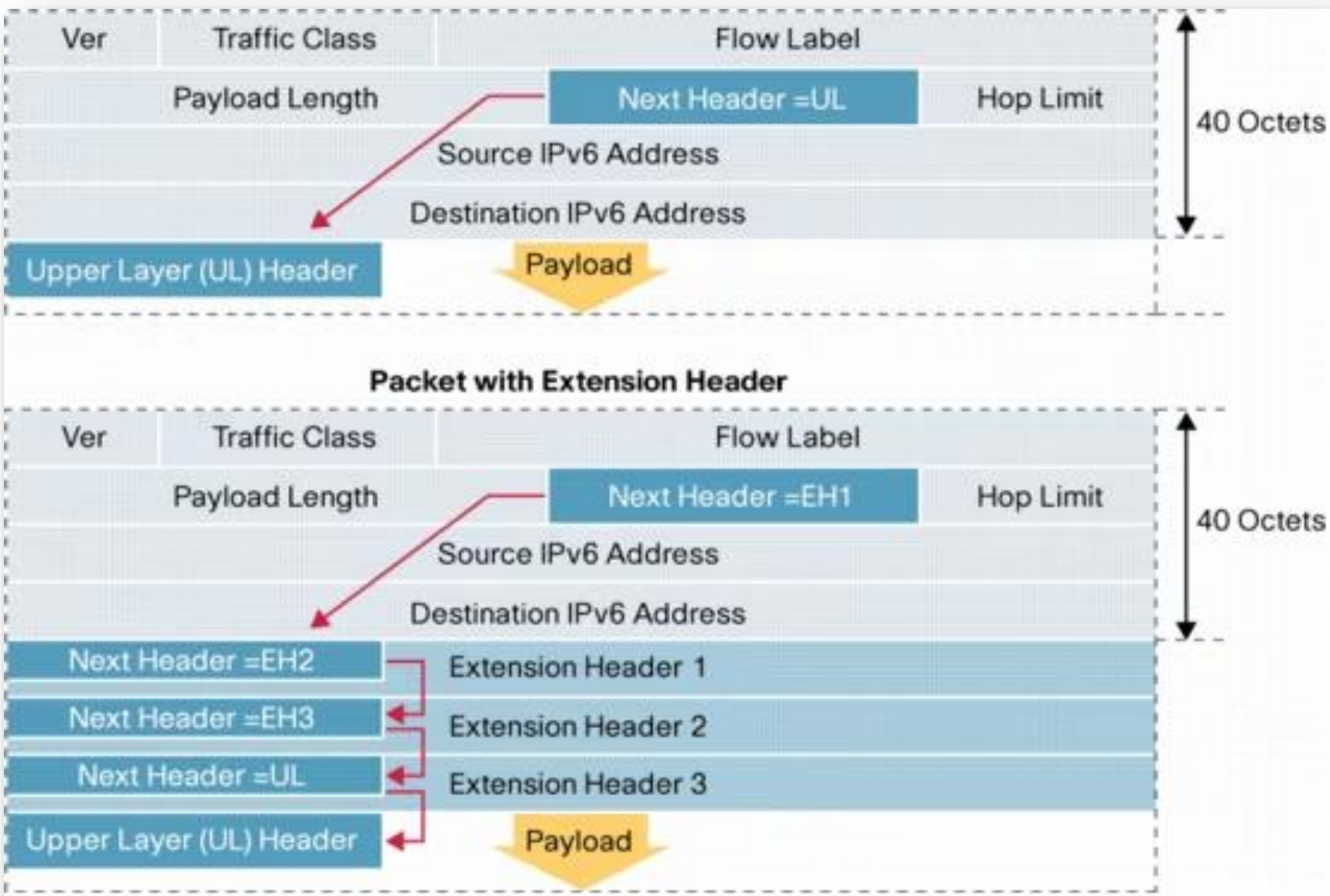
- The **Next Header** **field** specifies either the **type** of the **first** **extension header** (if any).
- Or the **upper-layer protocol** in the **payload** such as *TCP, UDP, or ICMPv6*(The field is similar to the IPv4 Protocol field).
- The **base headers** in **IPv6** store only the information which is **necessary**, instead of the information that is **rarely used** or **not needed.**
- All this **rarely used** or not required **information** is **stored** in the form of the **extension header** and placed between the **base header** and the **upper header.**
- A **distinct value** is used for the **identification** of the **extension header type.**
- In the **IPv6 header format**, the **Base Header's** next header **points** to the **header** that is the **first extension header**, when the extension header is used.

IPv6 Base Header

- After this, if one or more header is present in the **extension header** then, the **next header field** of the **first extension header** points to the **second extension header** and follows this process for the rest of the extension headers.
- The **next header field** of the **last extension header** points to the **Upper Layer header.**
- **Extension header types** are:

Extension Header	Description
Hop by Hop Options	All the devices that are present on the path examine this
Destination Options (with routing options)	Packet's destination examine this
Routing Header	Methods for taking the routing decision.
Fragment Header	Contains fragmented datagram parameters
Authentication Header	Authenticity verification
Encapsulation Security Payload	Encrypted data is carried by this

IPv6 Base Header

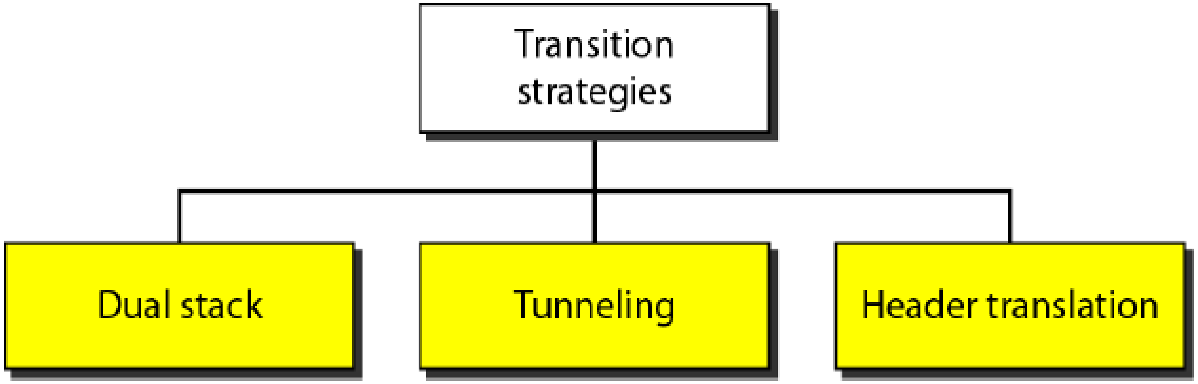


IPv6 Base Header

- **Hop limit**
  - This **8-bit** hop limit field serves the same purpose as the **TTL** field in **IPv4.**
- **Source address**
  - The **source address** field is a **16-byte** (128-bit) Internet address that identifies the original **source** of the datagram.
- **Destination address**
  - The **destination address** field is a **16-byte** (128-bit) Internet address that usually identifies the final **destination** of the datagram.

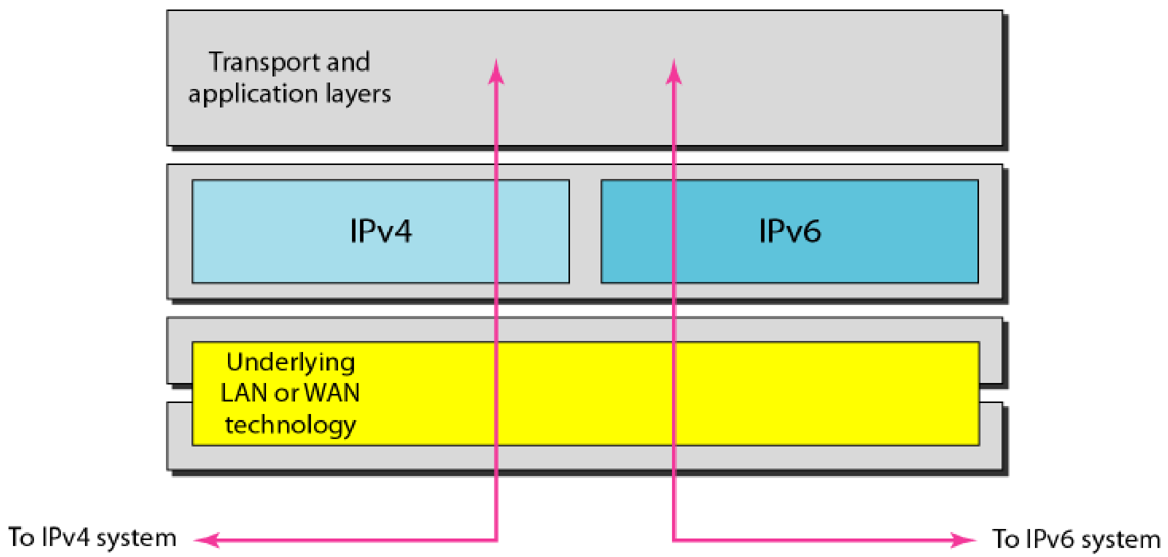
TRANSITION FROM IPv4 TO IPv6

- Because of the **huge number of systems** on the **Internet**, the **transition from IPv4 to IPv6 cannot happen suddenly.**
- It takes a **considerable amount of time** before every system in the Internet can **move from IPv4 to IPv6**.
- The **transition** must be **smooth** to prevent any problems between **IPv4** and **IPv6** systems.
- **Three strategies** have been devised by the **IETF** to help the **transition.**

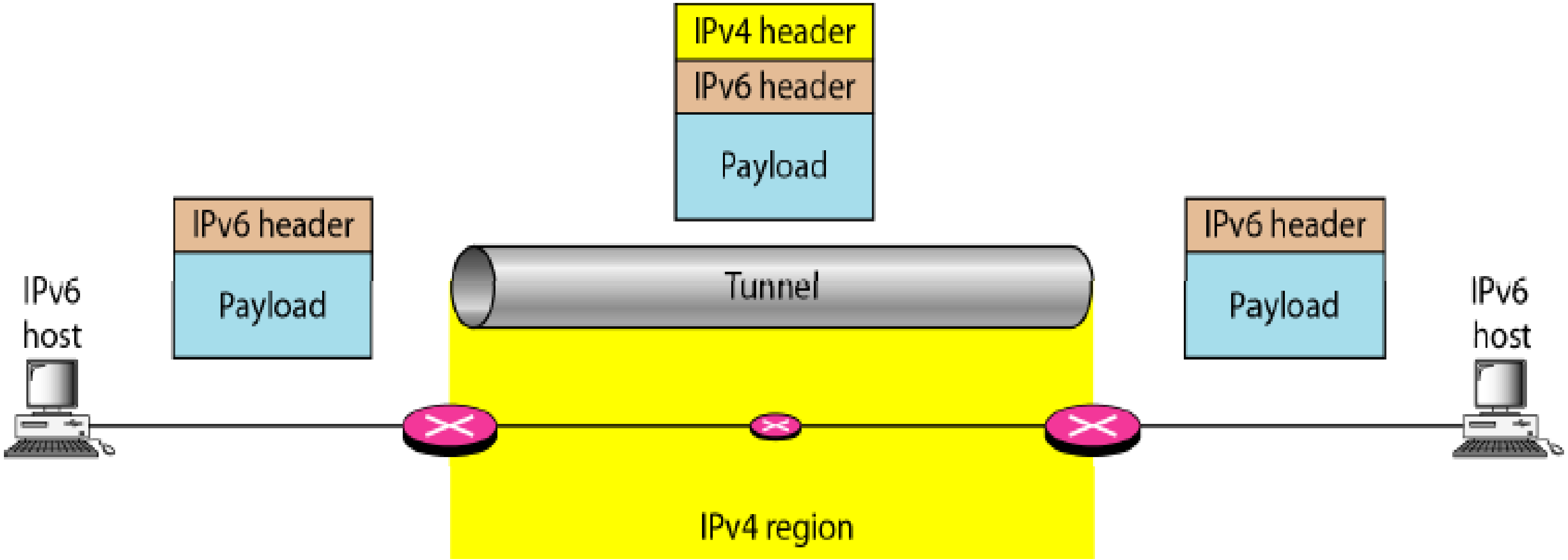


Dual Stack

- It is recommended that all hosts, before **migrating completely** to **version 6,** have a **dual stack** of protocols.
- In other words, a station must run **IPv4 and IPv6 simultaneously until all the Internet uses IPv6**.
- To determine **which version** to use when sending a packet to a destination, the source host **queries** the **DNS**. If the DNS returns an **IPv4 address**, the source host sends an IPv4 packet. If the DNS returns an **IPv6 address**, the source host sends an **IPv6 packet.**



Tunneling

- **Tunneling** is a strategy used when **two computers** using **IPv6** want to communicate with each other and the packet must pass through a **region that uses IPv4.**
- To pass through this **region,** the **packet must have an IPv4 address**.
- So the **IPv6 packet** is **encapsulated** in an **IPv4 packet** when it enters the region, and it **leaves its capsule when it exits** the region.
- 

Header Translation

- **Header translation** is necessary when the **majority of the Internet has moved to IPv6** but **some systems still use IPv4**.
- The **sender** wants to use **IPv6**, but the **receiver** does **not understand IPv6**.
- **Tunneling does not work** in this situation because the packet must be in the **IPv4 format** to be understood by the **receiver.**
- In this case, the **header format must be totally changed** through **header translation**. The **header** of the **IPv6 packet** is **converted** to an **IPv4 header.**