COMPUTER COMMUNICATION NETWORKS

M Rajasekar

Department of Electronics and Communication Engineering

IPv6: Datagram format, Transitioning from IPv4 to IPv6 & ICMP

M Rajasekar
Department of Electronics and Communication Engineering

IPv6: Datagram format, Transitioning from IPv4 to IPv6

IPv6 or Internet Protocol version 6

- Proposed by IETF (actually started to address the limitations of IPv4)
- Initiated in 1998 and came into effect on 6 June 2012
- Provides 3.4×10^{38} IP addresses of 128 bits each
- Currently implemented by new ISPs and carriers
- About 22% of the IP traffic is due to IPv6 as of 2018
- Fixed 40 byte header compared to the 20 byte (variable length) IPv4 header
- It is more robust to IP spoofing and attacks
- Besides unicast and multicast (IPv4 modes), supports anycast communications

IPv6: Datagram format, Transitioning from IPv4 to IPv6

IPv6 addressing:

- 128 bit number split into eight 16 bit blocks which are in turn converted into hexadecimal numbers and separated by colons
- Example:

```
0010000000000001 0000000000000000 0011001000111000
1101111111100001 0000000001100011 0000000000000000
0000000000000000 1111111011111011
```

```
2001:0000:3238:DFE1:0063:0000:0000:FEFB
```

- Rule 1: Discard leading zeros

```
2001:0000:3238:DFE1:63:0000:0000:FEFB
```

IPv6 addressing:

- Rule 2: Two or more blocks of consecutive zeros can be replaced by ::
  - ➢ Rule 2 is exercised only once
  - ➢ A single block of zeros can be simply replaced by 0

2001:0000:3238:DFE1:63:0000:0000:FEFB

2001:0000:3238:DFE1:63::FEFB

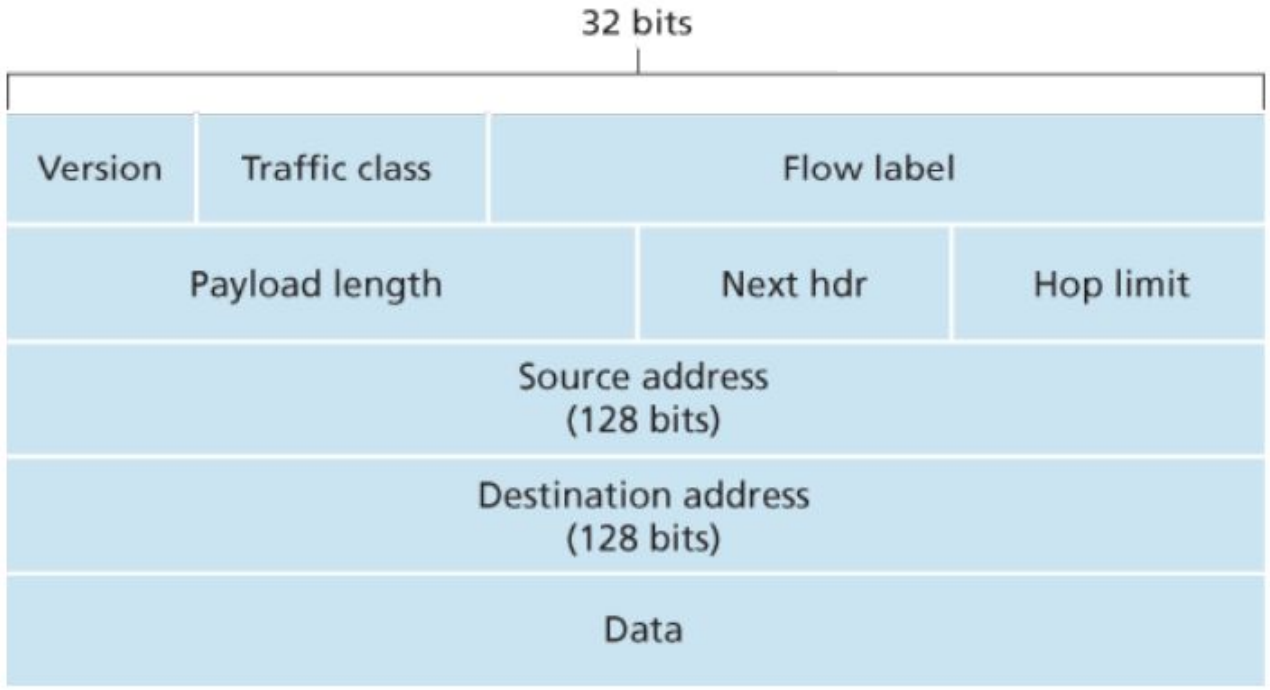
2001:0:3238:DFE1:63::FEFB

- Each IPv6 address can be viewed as network prefix (64 bits) followed by interface ID (64 bits)

IPv6 addressing:

- Prefixed with special meaning
- Link local address (FE80::/10 or 1111 1110 10) can be formed by
- Global unicast (2000::/3 or 0010)
- Multicast address (FF00::/8 or 1111 1111)
- Unique local address (FC00::/7)

IPv6: Datagram format



Key differences with IPv4

Doesn't have:
options, header length, internet checksum and datagram fragmentation

Has:
128 bit IP addresses,
flow label and payload length

IPv6: Datagram format

Version: This 4-bit field identifies the IP version number. Not surprisingly, IPv6 carries a value of 6 in this field.

Traffic class: The 8-bit traffic class field, like the TOS field in IPv4, can be used to give priority to certain datagrams within a flow, or it can be used to give priority to datagrams from certain applications

Flow label: This 20-bit field is used to identify a flow of datagrams.

Payload length: This 16-bit value is treated as an unsigned integer giving the number of bytes in the IPv6 datagram following the fixed-length, 40-byte datagram header.

IPv6: Datagram format

Next header: This field identifies the protocol to which the contents (data field) of this datagram will be delivered (for example, to TCP or UDP). The field uses the same values as the protocol field in the IPv4 header.

Hop limit: The contents of this field are decremented by one by each router that forwards the datagram. If the hop limit count reaches zero, the datagram is discarded.

Source and destination addresses: The various formats of the IPv6 128-bit address are described in RFC 4291.

Data: This is the payload portion of the IPv6 datagram. When the datagram reaches its destination, the payload will be removed from the IP datagram and passed on to the protocol specified in the next header field.

Transitioning from IPv4 to IPv6 (described in RFC 4213)

How will network operate with mixed IPv4 and IPv6 routers?

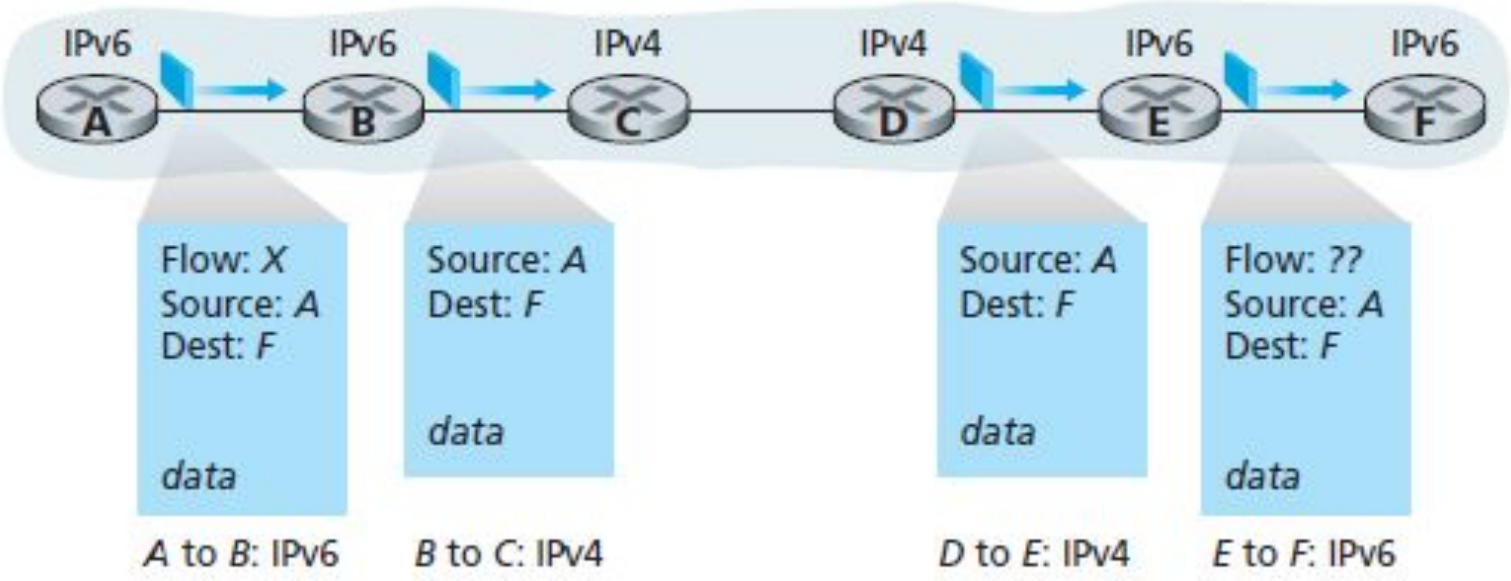
- The new IPv6- capable systems can be made backward-compatible, that is, can send, route, and receive IPv4 datagrams,
- But the already deployed IPv4-capable systems are not capable of handling IPv6 datagrams.

- The two approaches for transition from IPv4 to IPv6
  - Dual stack approach
  - Tunneling

IPv6: Datagram format, Transitioning from IPv4 to IPv6

Transitioning from IPv4 to IPv6 (described in RFC 4213)

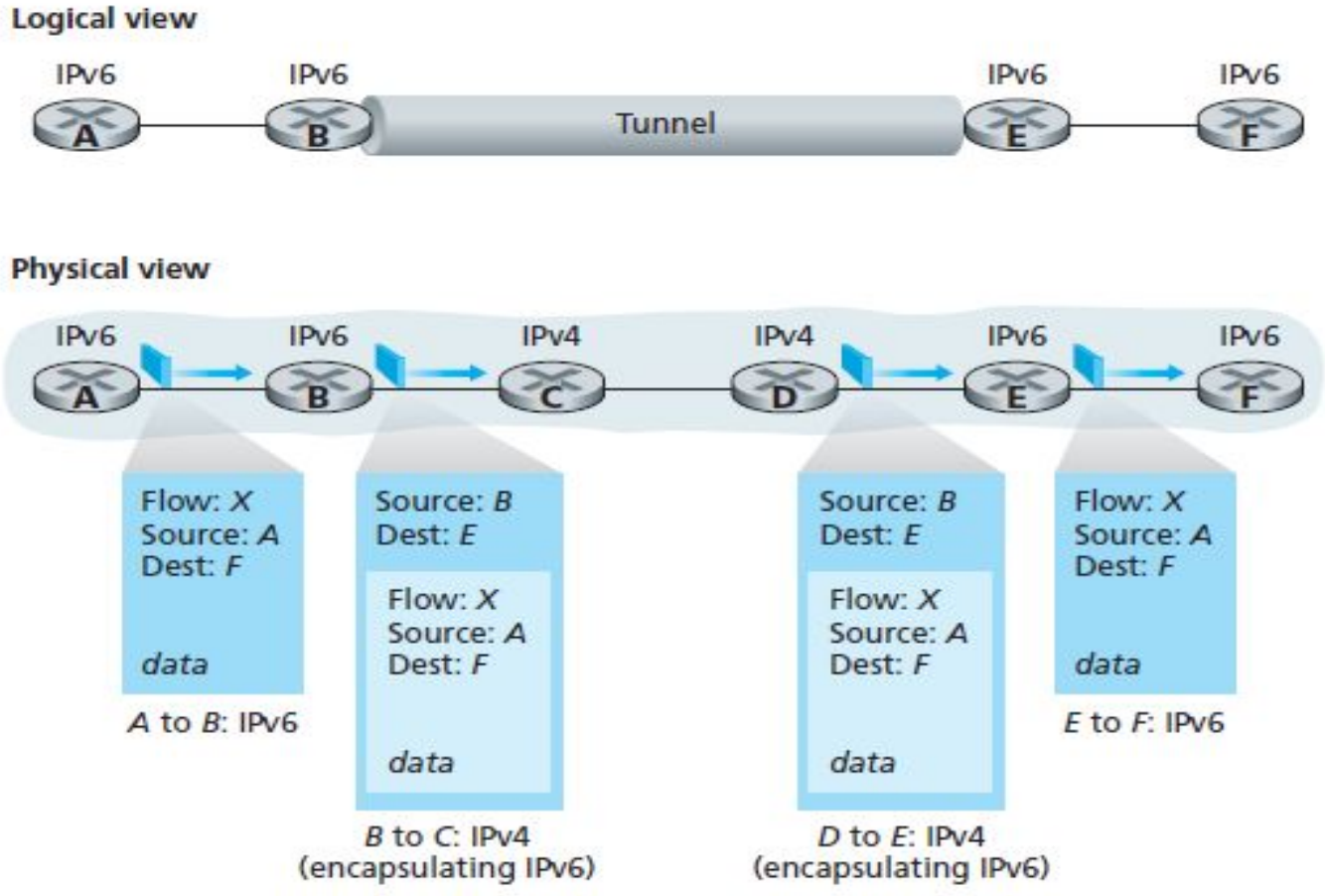
- **Dual stack approach**
  - Special nodes capable of forwarding both IPv4 and IPv6 packets.
  - Hosts can communicate using IPv6 only if all routers support IPv6
  - Proof by contradiction (figure below)



IPv6: Datagram format, Transitioning from IPv4 to IPv6

Transitioning from IPv4 to IPv6 (described in RFC 4213)

- **Tunneling approach**



Transitioning from IPv4 to IPv6 (described in RFC 4213)

- **Tunneling approach- Numerical**

http://gaia.cs.umass.edu/kurose_ross/interactive/ip_tunneling.php

ICMP – Internet Control Message Protocol

- ICMP is used by network devices, including routers, to send error messages and operational information
- Defined in RFC792
- Messages are generated by IP software and not user process
- Typical use of ICMP is error reporting.
- Some of the common ICMP messages
  - Network not reachable
  - TTL expired
  - Destination port not reachable
  - Echo and Echo reply

ICMP – Internet Control Message Protocol (Contd..)

- ICMP messages are carried inside IP datagrams
- E.g. The ping program sends an ICMP **type 8 code 0** message to the specified host.

The destination host, seeing the echo request, sends back a **type 0 code 0** ICMP echo reply.

ICMP – Internet Control Message Protocol (Contd..)

ICMP Type	Code	Description
0	0	echo reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench (congestion control)
8	0	echo request
9	0	router advertisement
10	0	router discovery
11	0	TTL expired
12	0	IP header bad

Figure 5.19 ICMP message types

THANK YOU

M Rajasekar

Department of Electronics and Communication Engineering

rajasekarmohan@pes.edu