CN-Basic
L29

IPv6 and IPSec

Dr. Ram P Rustagi
rprustagi@ksit.edu.in
http://www.rprustagi.com
https://www.youtube.com/rprustagi

IPv6 Resources

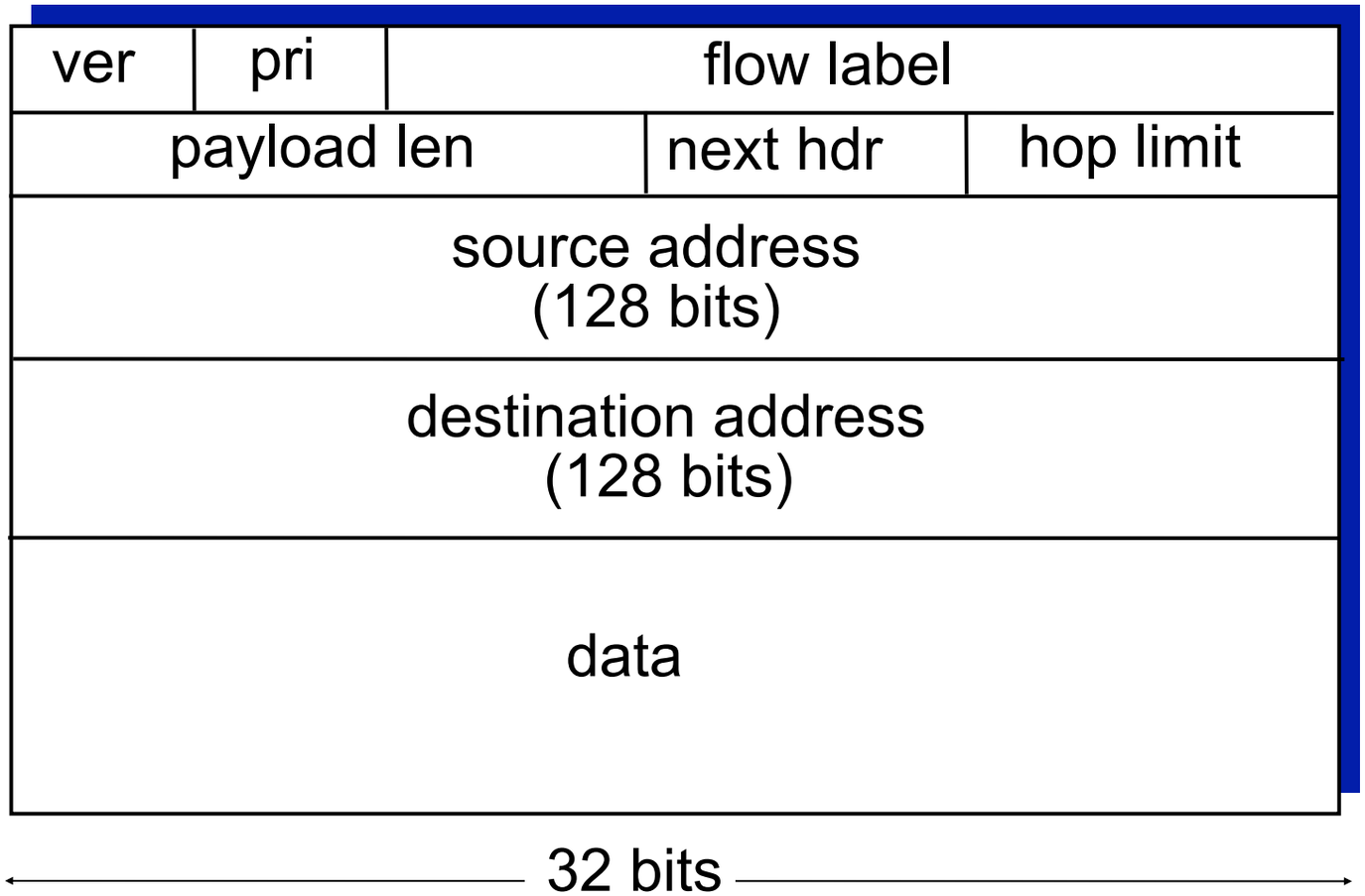
- http://www.ipv6forum.org/dl/books/the_second_internet.pdf
- http://www.ipv6forum.org/dl/books/ipv6forall.pdf http://www.6deploy.eu/e-learning/english/
- http://highered.mcgraw-hill.com/sites/0073376221/student_view0/chapter22/java_applets.html

IPv6 - Why New IP/Motivation

- More addresses needed
- Billion of new devices
  - May explode by 100 times
  - Pervasive computing (internet of devices, things)
- Billions of new users: India, China etc
- Ability to do end to IPSec
  - NAT not needed
- additional motivation:
  - header format helps speed processing/forwarding
  - header changes to facilitate QoS
  - fixed-length 40 byte header
  - no fragmentation allowed

IPv6 datagram format

priority: identify priority among datagrams in flow
flow Label: identify datagrams in same "flow."
(concept of"flow" not well defined).
next header: identify upper layer protocol for data

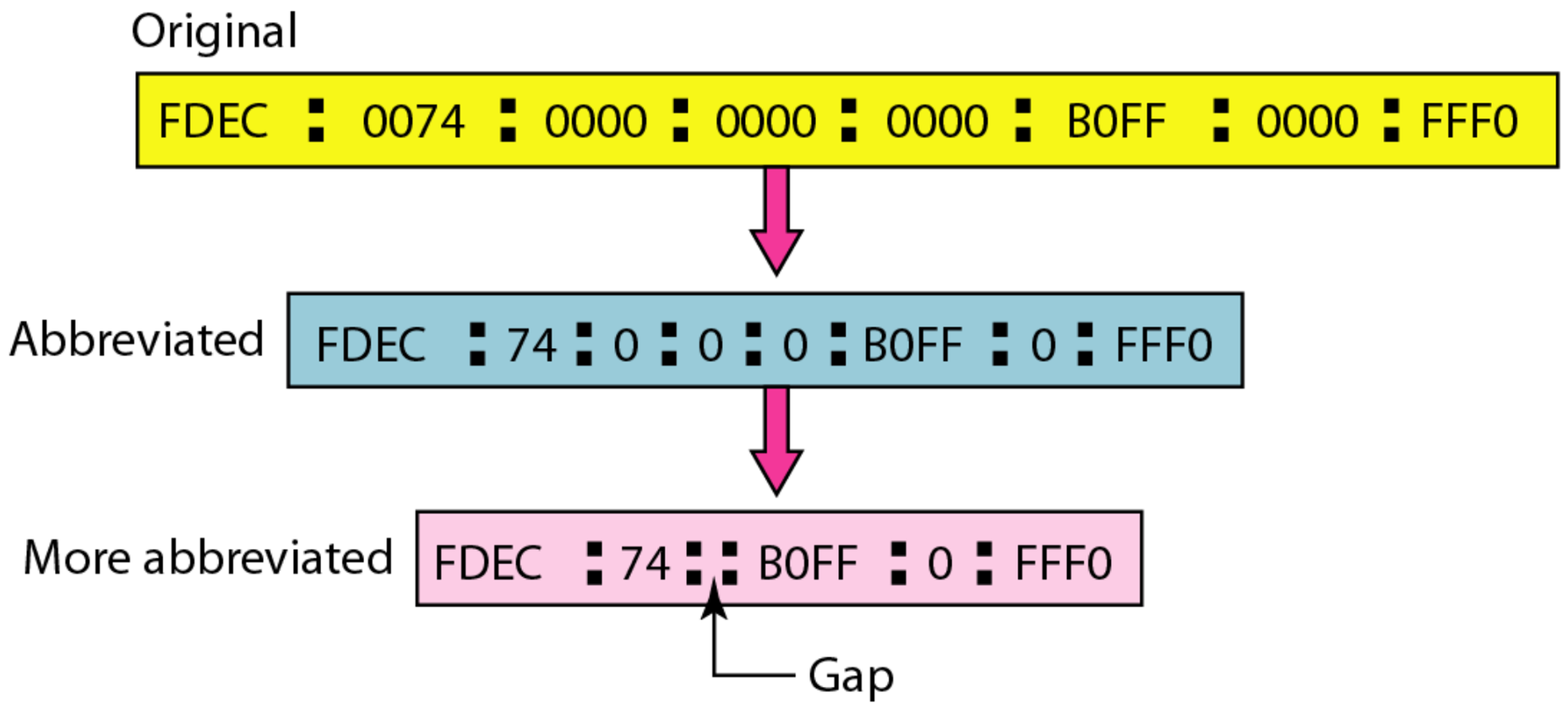


Other changes from IPv4

- *checksum:* removed entirely to reduce processing time at each hop
  - better header format
- *options:* allowed, but outside of header, indicated by "Next Header" field
- *ICMPv6:* new version of ICMP
  - additional message types, e.g. "Packet Too Big"
  - multicast group management functions
  - allows for extension of protocols
- Security & Mobility support

IPv6 Addresses

- 128 bits address
  - 16 bytes = 32 hex digits
- Written in hexadecimal colon notation
  - preferred form - x:x:x:x:x:x:x:x



- Src: Frozen Computer Networking

IPv6 Address Types

- Unicast
  - aggregatable with prefixes of arbitrary length
- Multicast
  - No broadcast in IPv6
  - Broadcast considered one special case of Multicast
  - uses special link local all nodes multicast group
    - FF02::1 - Analogous to 224.0.0.1
    - FF02::2 - link local scope all routers
- Anycast
  - packets delivered to one member of group

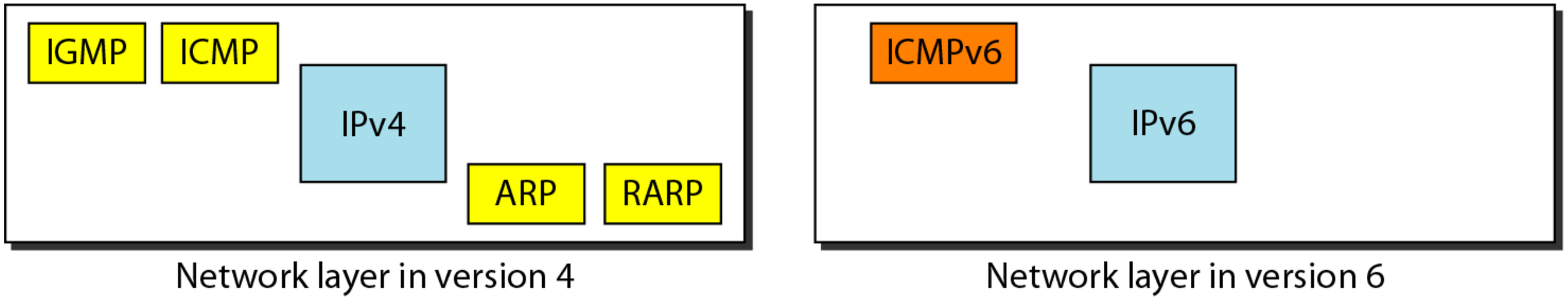
IPv6 Address Allocation

- Unicast
  - Global Unicast (First 3 bits are `001`)
  - Site-local unicast (deprecated) (0xFEC0)
  - Link-local unicast (0xFE80)
  - Unique local (`(0xFC)`
    - like `192.168.x.x, 172.16.x.x-172.31.x.x, 10.x.x.x`
- Global Unicast
  - For one to one communication between hosts
    - global routing prefix
    - subnet identifier
    - interface identifier
      - similar to hostid in IPv4

IPv6 Address - Special Addresses

- The Unspecified Address
  - `0:0:0:0:0:0:0:0`
  - can be written as `::`
- The loopback address
  - `0:0:0:0:0:0:0:1`
  - `can be written as ::1`
  - similar to `127.0.0.1` in IPv4

ICMPv6



- ICMPv6 is more complicated than ICMPv4
  - ARP and IGMP are combined into ICMPv6
  - More messages have been added
- ICMPv6 Message categories
  - Error Messages
  - Informational Messages
  - Neighbor Discovery Messages
    - ND (Neighbor Discovery) protocol
  - Group Membership messages
    - MLD (Multicast Listener Delivery) protocol

ICMPv6 Messages

- Stateless Autoconfiguration
  - RFC 2462
  - allows a host to generate its own address
  - uses local information and router advertisement info
  - routers advertise the prefix identifying the subnets
  - host generates the interface id within the subnet
  - when router is absent
    - host generates link local address
    - permits communication on same link
  - applies only to hosts and not to routers
    - routers need to be configured by some other means

Transition from IPv4 to IPv6

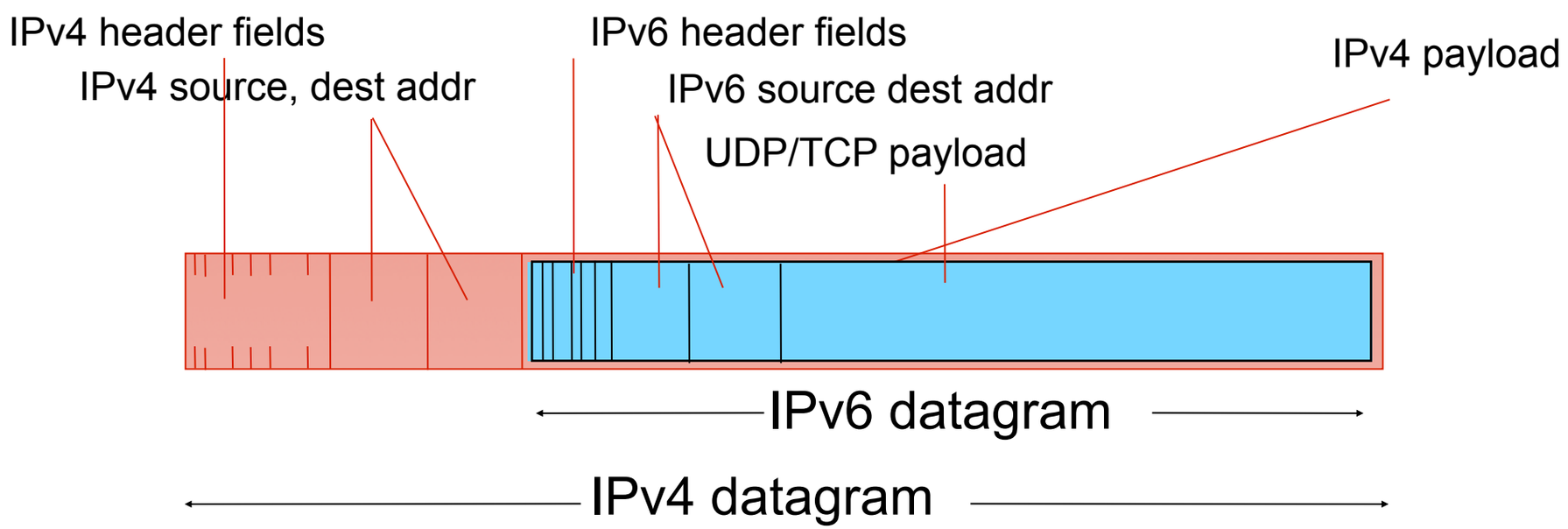
- Not all routers can be upgraded simultaneously
  - no "flag days"
  - how will network operate with mixed IPv4 and IPv6 routers?
- Transition Strategies
  - Dual Stack
  - Tunneling
  - Address Translation

Transition from IPv4 to IPv6

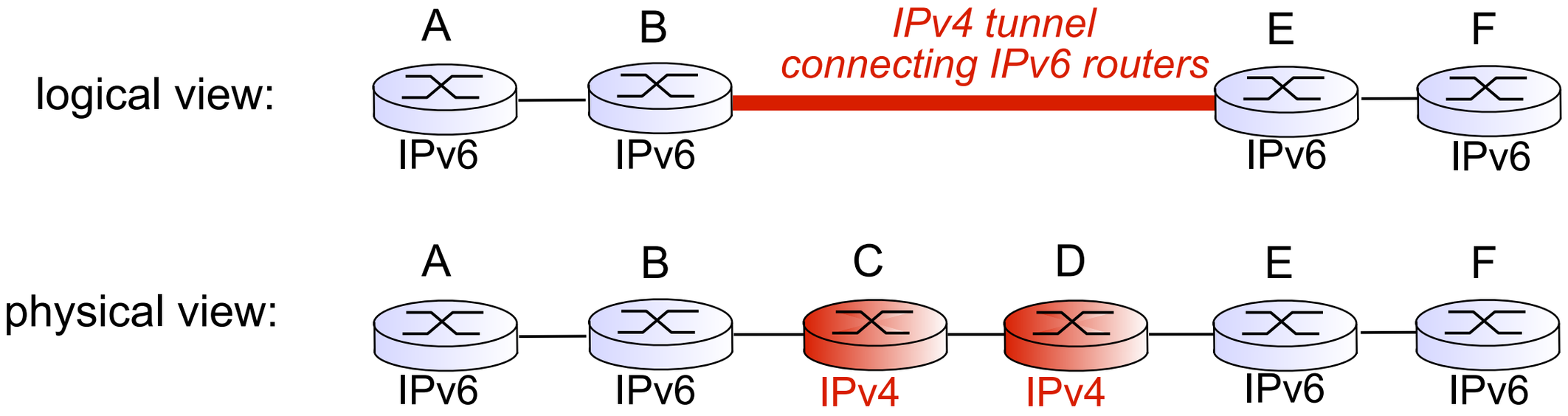
- Dual Stack
  - at network layer, both IPv4 and IPv6 present
  - DNS response determines which stack to use
    - response can IPv4 or IPv6 or both
      - If IPv6 is present, use IPv6
      - Else use IPv4
  - Two stacks co-exist indefinitely
  - Bundled with OS, no extra add on software/cost
    - Linux, Mac, Windows (including Windows XP)
  - No change in Datalink layer/Transport layer

Transition from IPv4 to IPv6

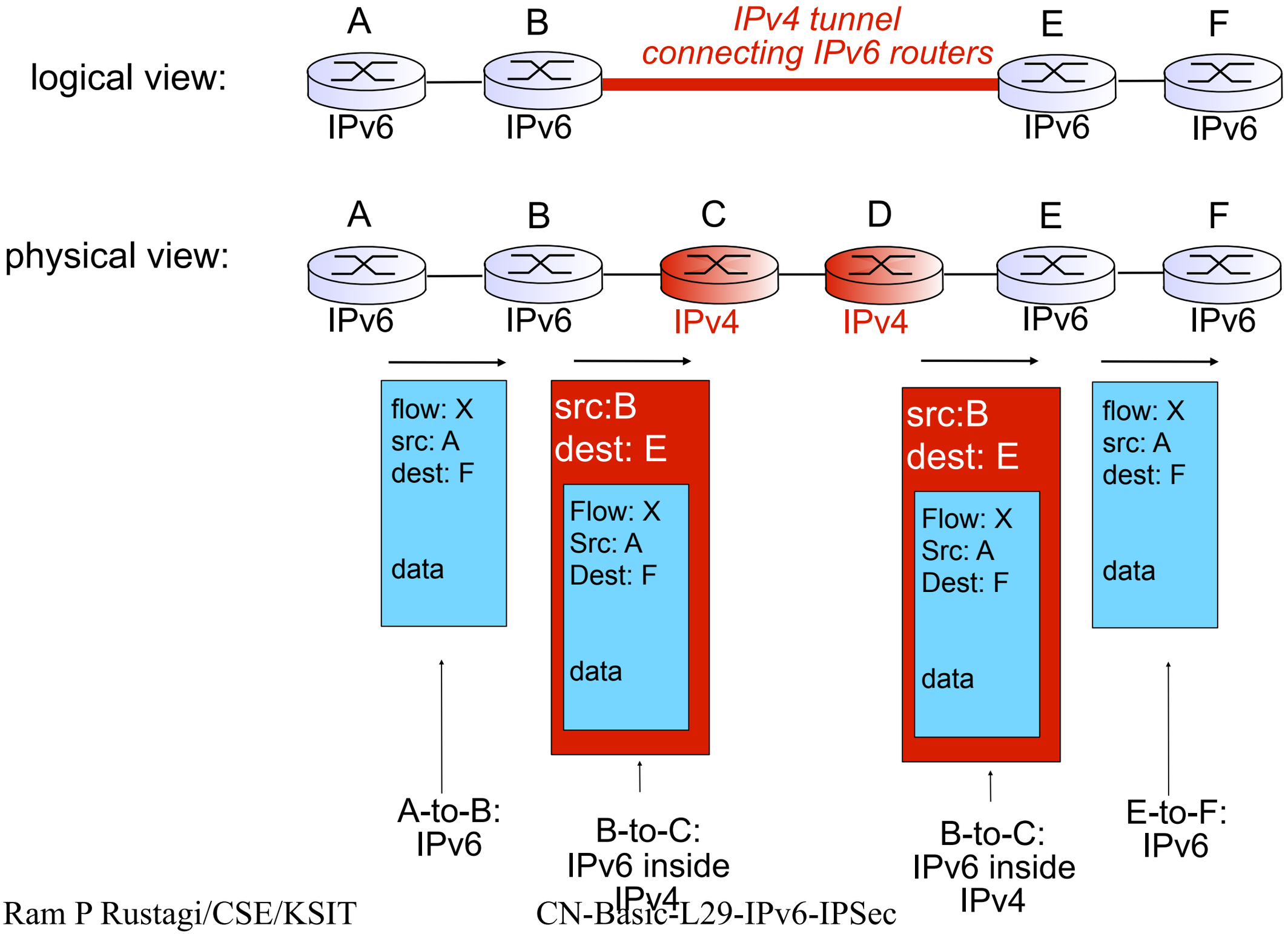
- *tunneling:* IPv6 datagram carried as *payload* in IPv4 datagram among IPv4 routers
  - similar to IP in IP tunnels
- There is no virtual connection setup
  - two end points need to be configured
- intermedia IPv4 routers treat it as IPv4 packet



Tunneling


logical view:
A
B
IPv4 tunnel
connecting IPv6 routers
E
F
IPv6
IPv6
IPv6
IPv6
physical view:
A
B
C
D
E
F
IPv6
IPv6
IPv4
IPv4
IPv6
IPv6

Tunneling


logical view:
A
B
IPv4 tunnel
connecting IPv6 routers
E
F
IPv6
IPv6
IPv6
IPv6
physical view:
A
B
C
D
E
F
IPv6
IPv6
IPv4
IPv4
IPv6
IPv6
flow: X
src: A
dest: F
data
src:B
dest: E
Flow: X
Src: A
Dest: F
data
src:B
dest: E
Flow: X
Src: A
Dest: F
data
flow: X
src: A
dest: F
data
A-to-B:
IPv6
B-to-C:
IPv6 inside
IPv4
B-to-C:
IPv6 inside
IPv4
E-to-F:
IPv6

Transition from IPv4 to IPv6

- Address Translation (NAT64)
  - provides full functionality when talking to IPv6
  - Normal/degraded functionality when talking to IPv4
  - IPv6 address is changed to IPv4 and vice versa
    - If mapped address, then use last 32 bits
  - The value of IPv6 priority, flow is discarded
  - TOS bits in IPv4 are set to 0
  - Checksum for IPv4 is computed and added
    - no checksum in IPv6
  - IPv6 extension headers compatible to IPv4 options
    - converted appropriately
  - Other IPv4 fields computed and inserted

IPSec

- IPv4 designed in 1970
  - No security support initially
- IPSec: Most populare secure network layer protocol
  - Widely deployed in VPNs
  - Backward compatible with IPv4 and IPv6
  - Can work with existing routers (w/o replacing these)
- IPSec can be end to end
  - Established between two hosts
  - No intermediate routers need to run IPSec
  - Works with both IPv4 and IPv6

IPSec Transport Mode

- Two end to end hosts establish IPSec session
  - Thus, IPSec is connection oriented
- All TCP and UDP run on top of IPSec
  - Enoys the support of security services provided by IPSec
  - IPSec encrypts the transport pkt on sender side
  - Encapsulates the resulting payload in IP datagram
  - Sends the payload in IPv4 datagram on internet
  - Destination host decrypts the payload, and gives to application

IPSec Transport Mode

- IPSec services
  - Cryptographic agreement
    - 2 hosts agree on cypto algorithm and keys
  - Encryption of IP datagram payload
    - Only receiving host can decrypt
  - Data integrity
    - Enables receiver to verify that header and encrypte data has not been tempered with.
  - Origin authentication (src IP in pkt is verified)
    - receiver is assured of sender's IP address
- Basically provides blanket services between 2 hosts
  - Both TCP and UDP protocols

IPv6 Summary

- Anycast, unicast, multicast addresses
- Auto configuration
- Colon Hexadecimal notation
- Destination option
- Dual Stack
- Extension headers
- Link Local addresses
- IPv4 compatible addresses
- Address translation

IPv6 Address

- Exercise 1
  - Given the address
    - 2001:0DB8:0000:CD30:0000:0000:0000:0000/60
  - which are correct representations
    - 2001:0DB8::CD30:0:0:0:0/60
    - 2001:0DB8:0:CD30::/60
    - 2001:0DB8:0:CD3/60
    - 2001:0DB8::CD30/60
    - 2001:0DB8::CD3/60

IPv6 Addresses

- Exercise 2
  - *Expand the address 0:15::1:12:1213 to its original*
- Answer
  - Align to the left side of double colon
  - Align to the right side of double colon
  - Fill the gaps with zeros

```
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
 0:   15:                    :    1:   12:1213
```

- The original address is

```
0000:0015:0000:0000:0000:0001:0012:1213
```

Src: Forouzan Computer Networking 4th edition