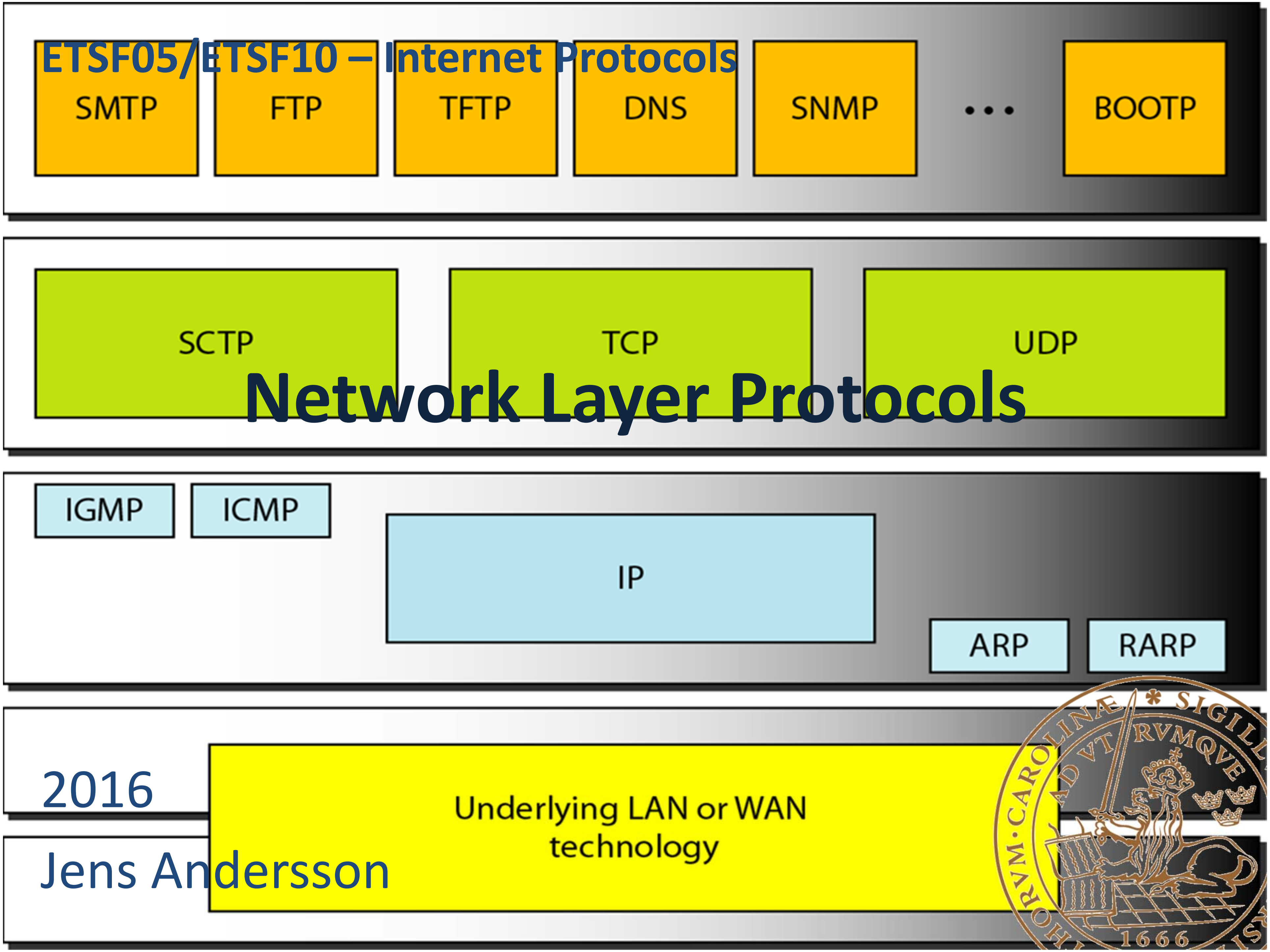
ETSF05/ETSF10 – Internet Protocols

Network Layer Protocols



2016

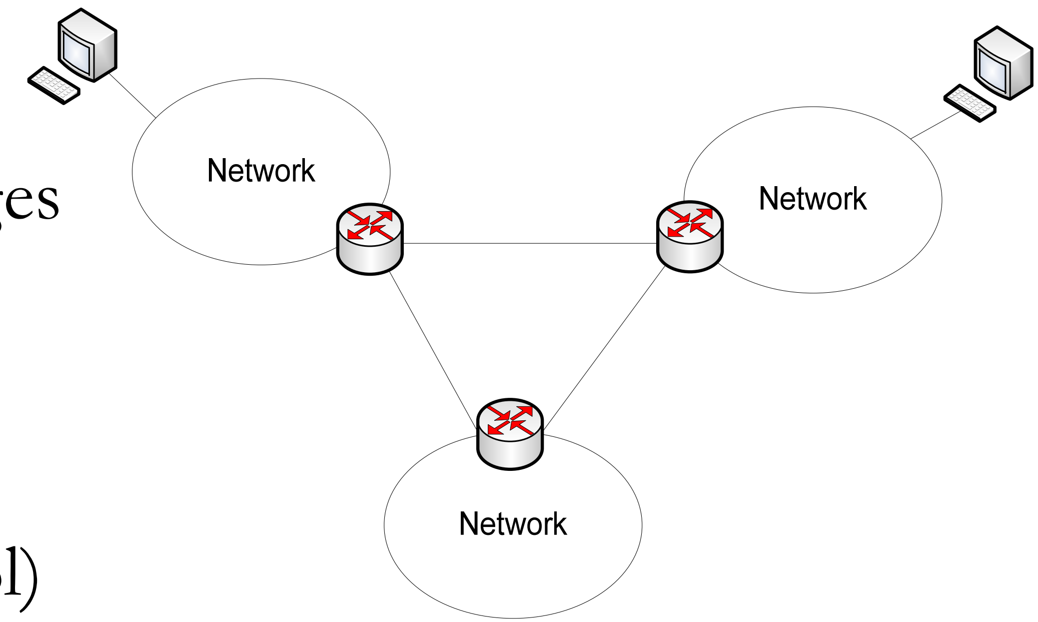
Jens Andersson

Agenda

- Internetworking
- IPv4/IPv6
- Framentation/Reassembly
- ICMPv4/ICMPv6
- IPv4 to IPv6 transition
- VPN/Ipsec
- NAT (Network Address Translation)

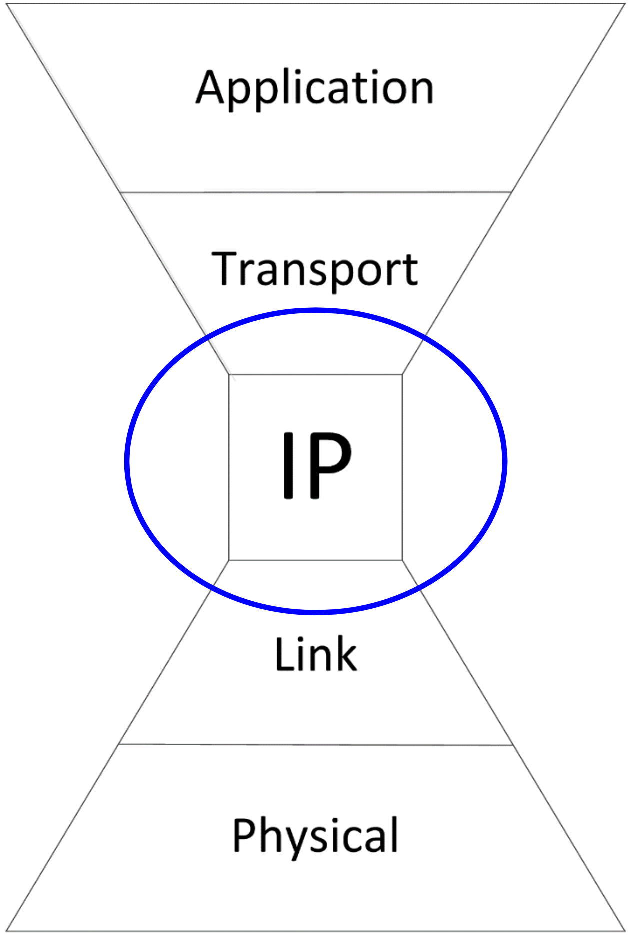
Basic idea of Kahn and Cerf's internetworking

- Host identification (Addresses)
- Forwarding of messages between networks (routing)
- End-to-end reliability (error and flow control)



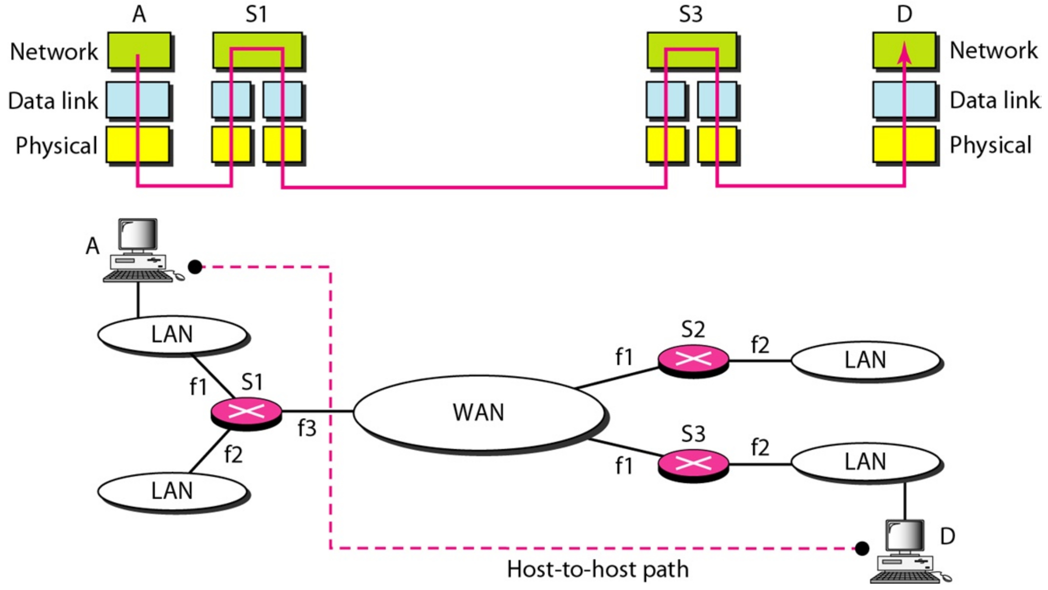
Connectionless Operation

- Internetworking involves connectionless operation at the level of the Internet Protocol (IP)
- Initially developed for the DARPA internet project
- IP specifies network addresses which is needed to access a particular network



Network layer

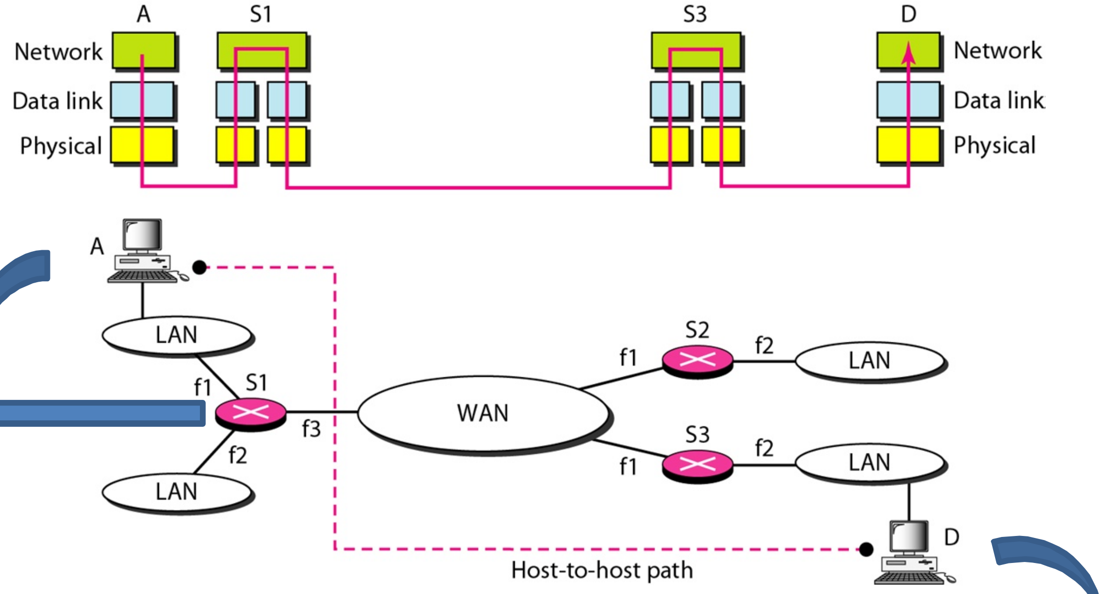
- L3 is end-to-end

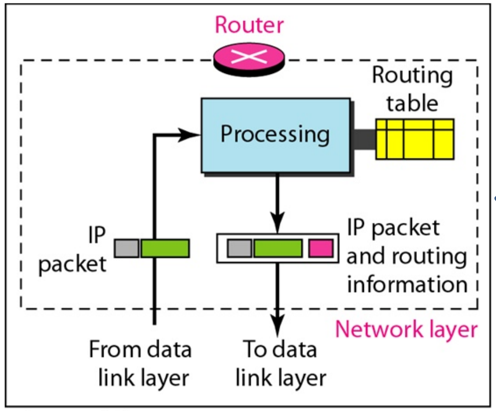


- L2 is host-to-host

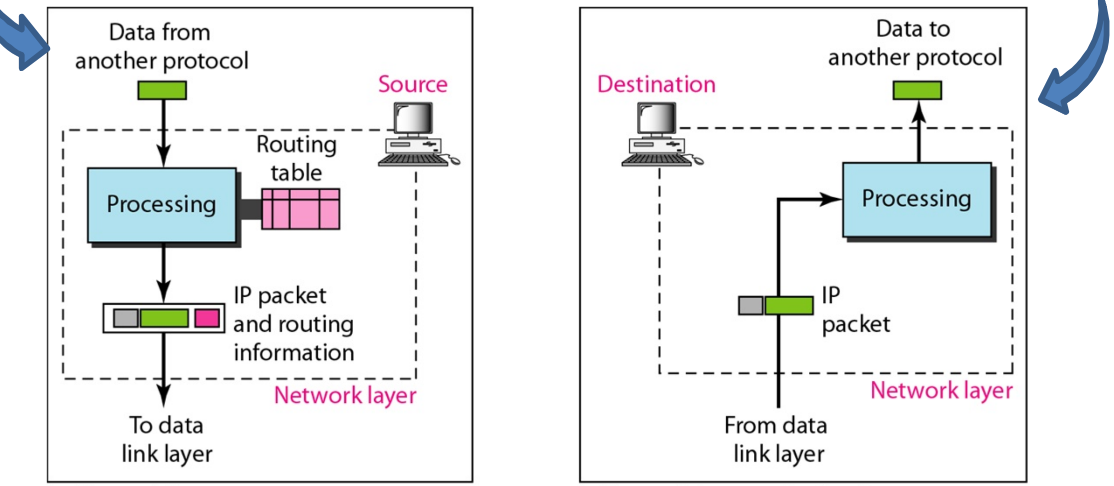
Network layer: Routing

- L3 is end-to-end





c. Network layer at a router



a. Network layer at source

b. Network layer at destination

Two functions:

❶ Addressing

❷ Feedback

Connectionless Internetworking

- IP provides a connectionless service between end systems
- Advantages:
  - Is flexible
  - Can be made robust
  - Does not impose unnecessary overhead
- Best Effort!

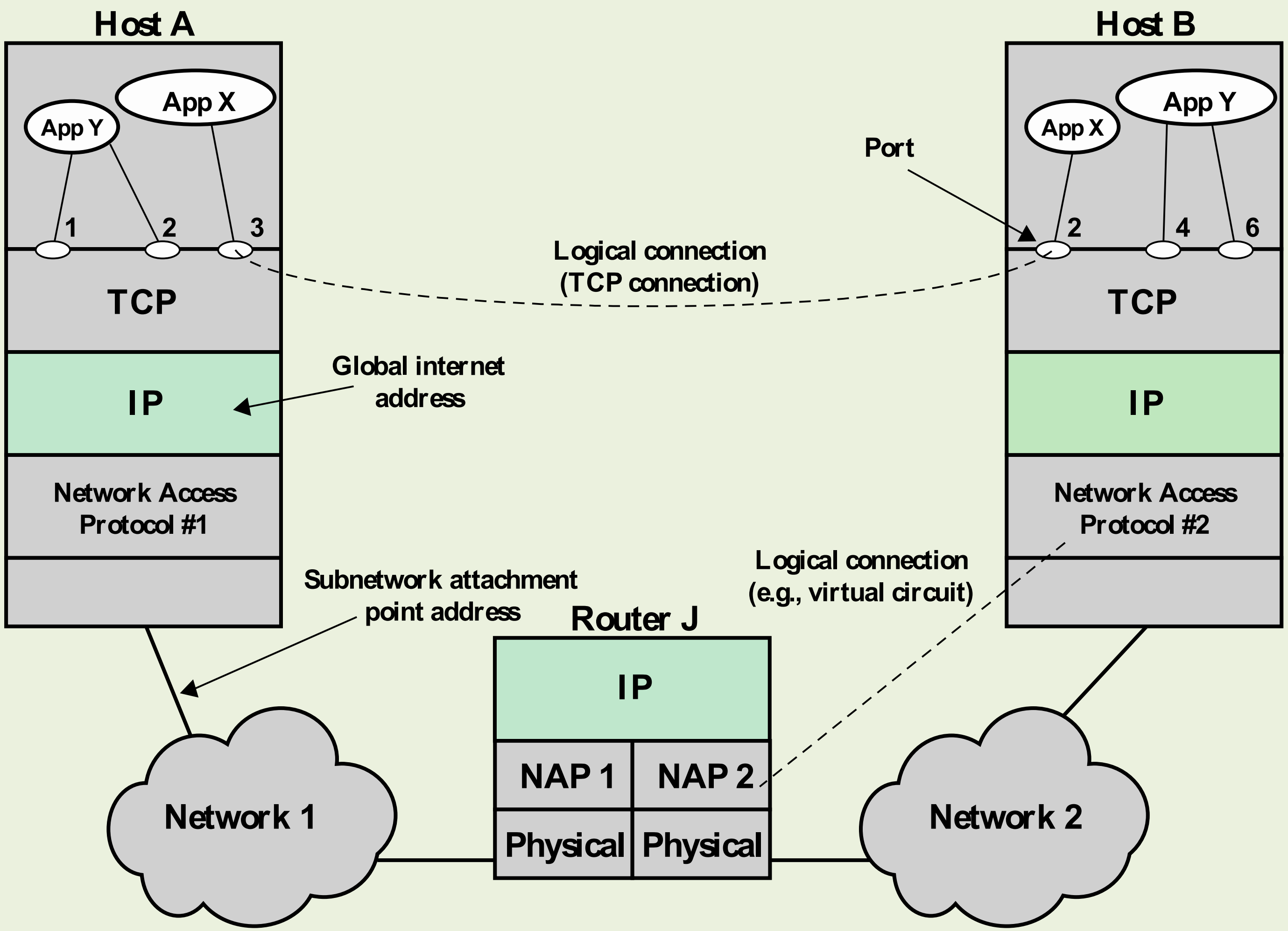


Figure 14.1 TCP/IP Concepts

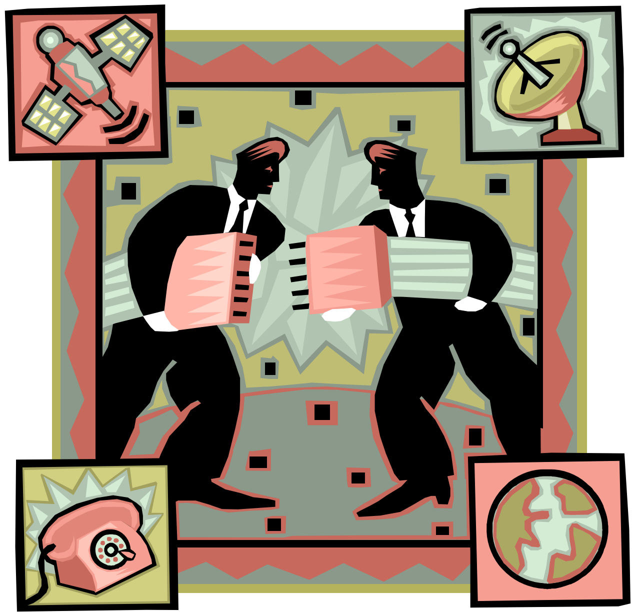
Internet Protocol (IP) v4

- Defined in RFC 791
- Part of TCP/IP suite
- Two specifications:

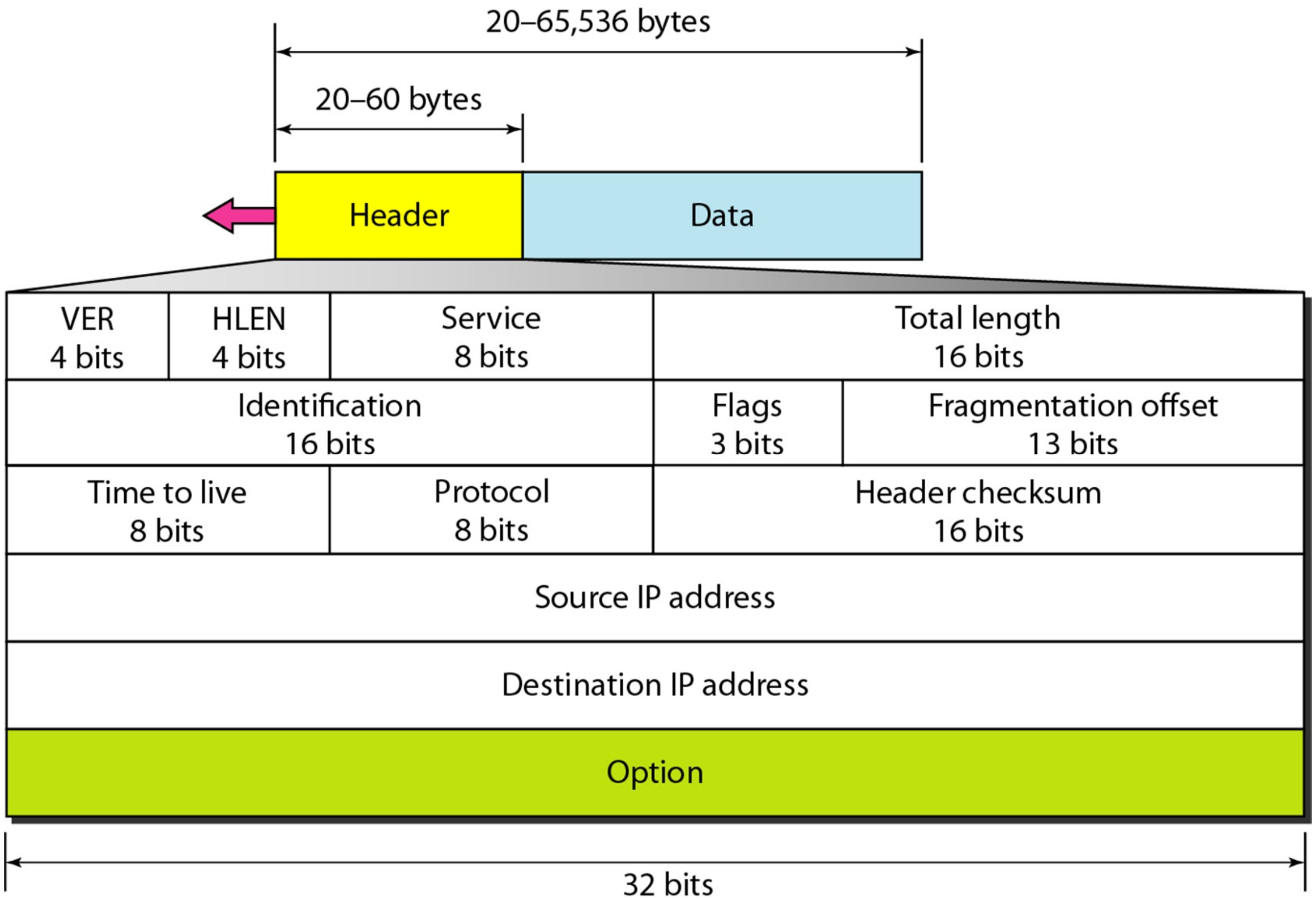
Specification of interface with a higher layer	Specification of actual protocol format and mechanisms

IPv4 Services in host

- Primitives
  - Specifies functions to be performed
  - Form of primitive implementation dependent
  - **Send:**
    request transmission of data unit
  - **Deliver:**
    notify user of arrival of data unit
- Parameters
  - Used to pass data and control information



IPv4 datagram



IPv4 Options

Security

Route recording

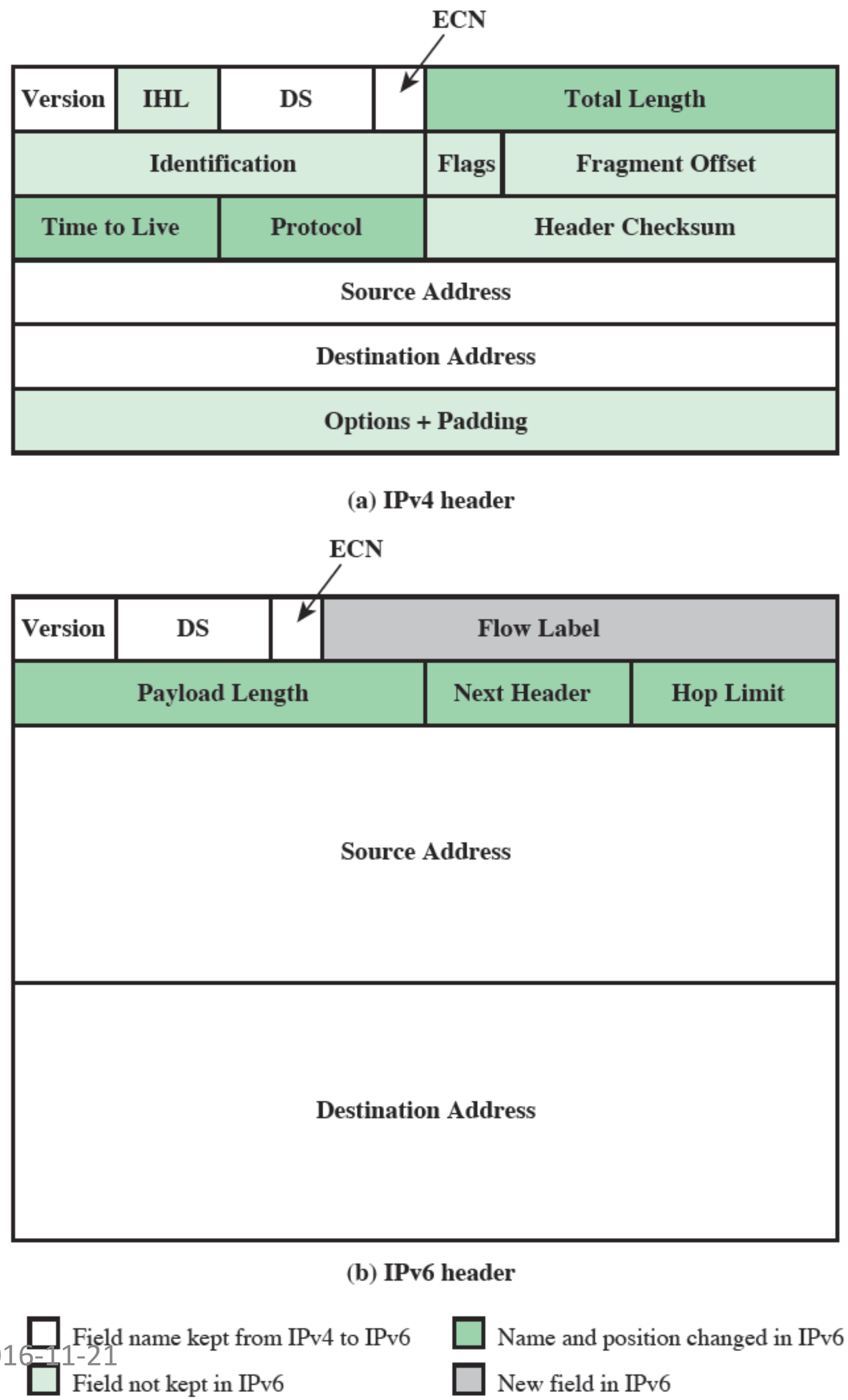
Source routing

Stream identification

Timestamping

Seldom/never used

- **Too weak**
- **Not working as intendent**
- **Security solved with IPsec**



IP and congestion control?!

- ECN =Explicit Congestion Notification field
- Notify any Transport Protocol (from router to end nodes) that this packet meets congestion
- Better alternative than just dropping a packet (Random Early Discard, transport layer lecture)

IP Next Generation

Address space exhaustion:

- Two level addressing (network and host) wastes space
- Network addresses used even if not connected
- Growth of networks and the Internet
- Extended use of TCP/IP
- Single address per host

Requirements for new types of service

- Address configuration routing flexibility
- Traffic support
- Security (IPsec built in)

IPv6 Enhancements

- Expanded 128 bit address space
- Improved option mechanism
  – Most not be examined by intermediate routes
- Dynamic address assignment
  – Address Auto Configuration (SL)AAC
- Increased addressing flexibility
  – Anycast and multicast
- Support for resource allocation
  – Labeled packet flows

IPv6 Header and Option Fields

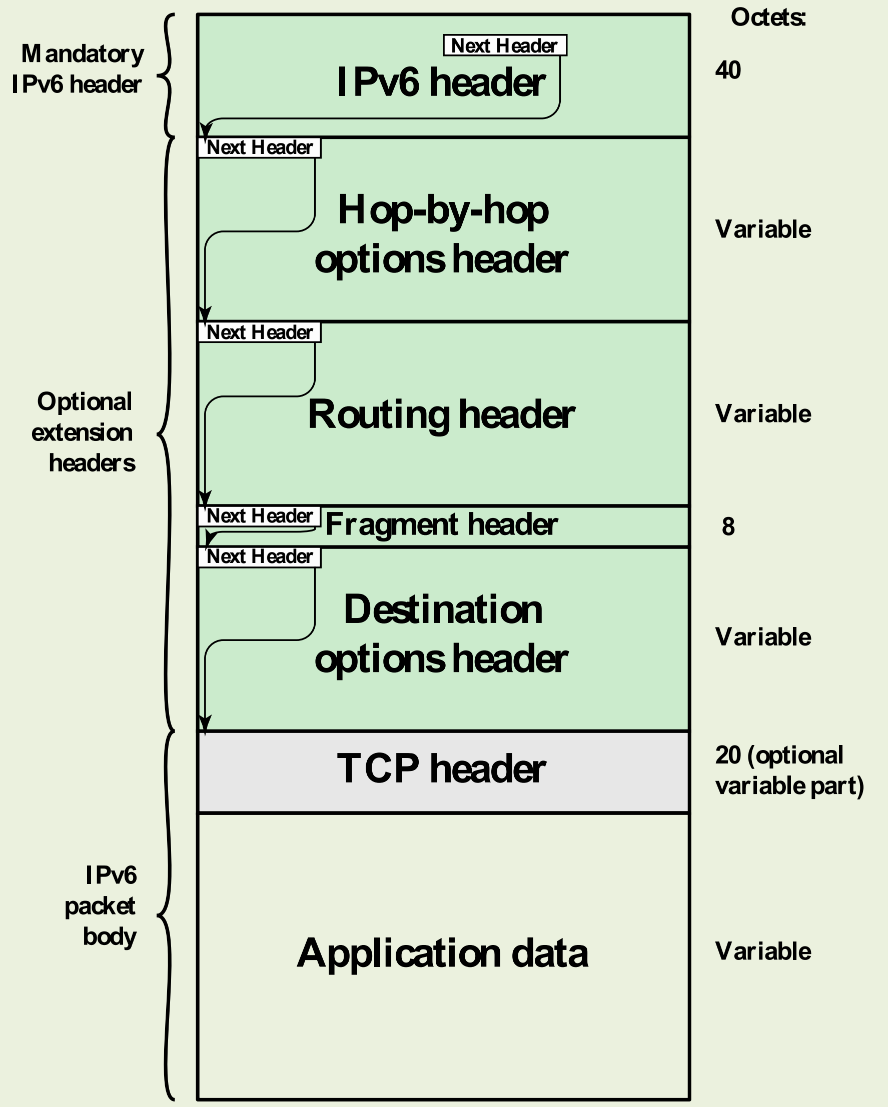
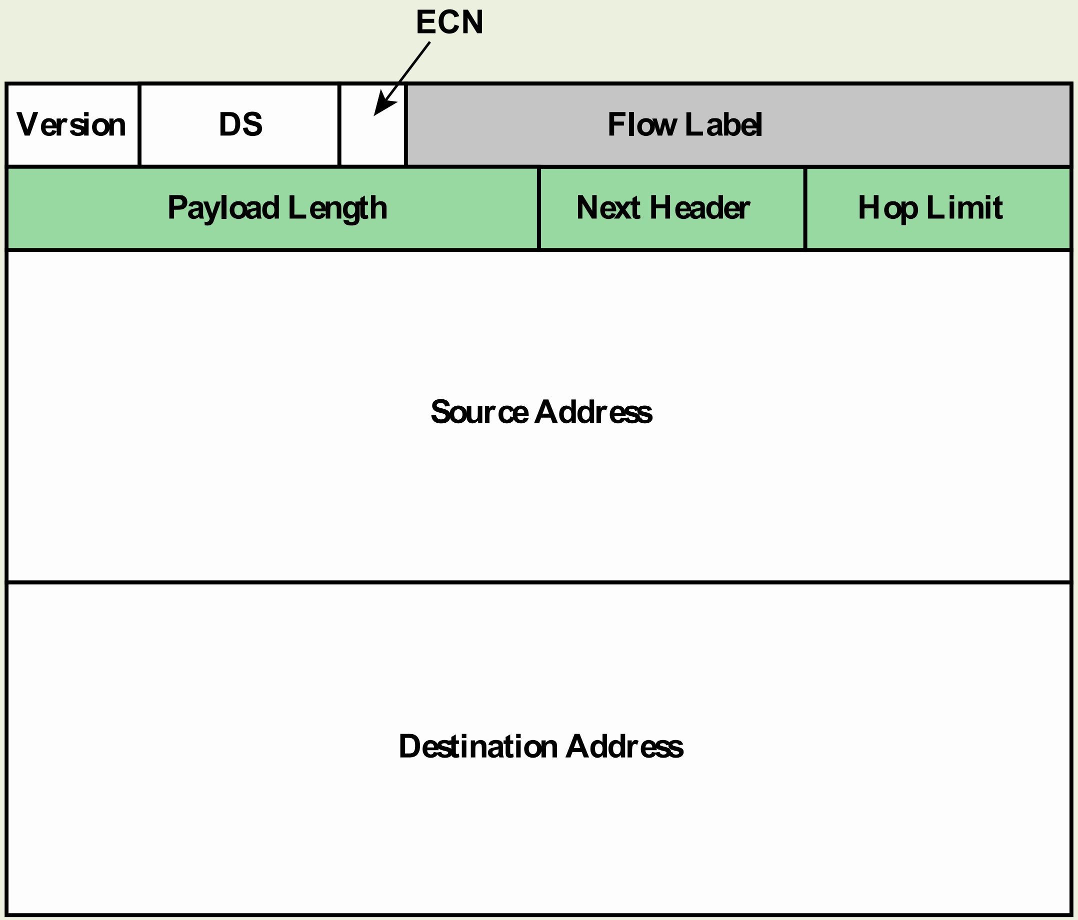


Figure 14.9 IPv6 Packet with Extension Headers (containing a TCP Segment)

IPv4 has option fields as part of single header -> header size varies



(b) IPv6 header

Field name kept from IPv4 to IPv6
Name and position changed in IPv6
Field not kept in IPv6
New field in IPv6

IPv6 Flow Label

Revert to Circuit Switched … ?

- Related sequence of packets that shall be treated as one entity
- Identified by source and destination address plus flow label
- Router treats packets in flow as sharing attributes
- May treat flows differently/individually
- Alternative to including all information in every header
- Have requirements on flow label processing

IPv6 and QoS

Flow label

- Identification of a stream
  - TCP sessions
  - Virtual connections
- Processing
  - Flow label table
  - Forwarding table
- Routing
  - Algorithms still necessary
  - But not run for every packet!

Traffic class

- Classification of packets
  - Queueing schemes
  - Relation to delay
- TCP vs. UDP
  - Congestion-controlled
  - Non-congestion-controlled
- Other protocols
  - RTP
  - RSVP

IPv6 Addresses

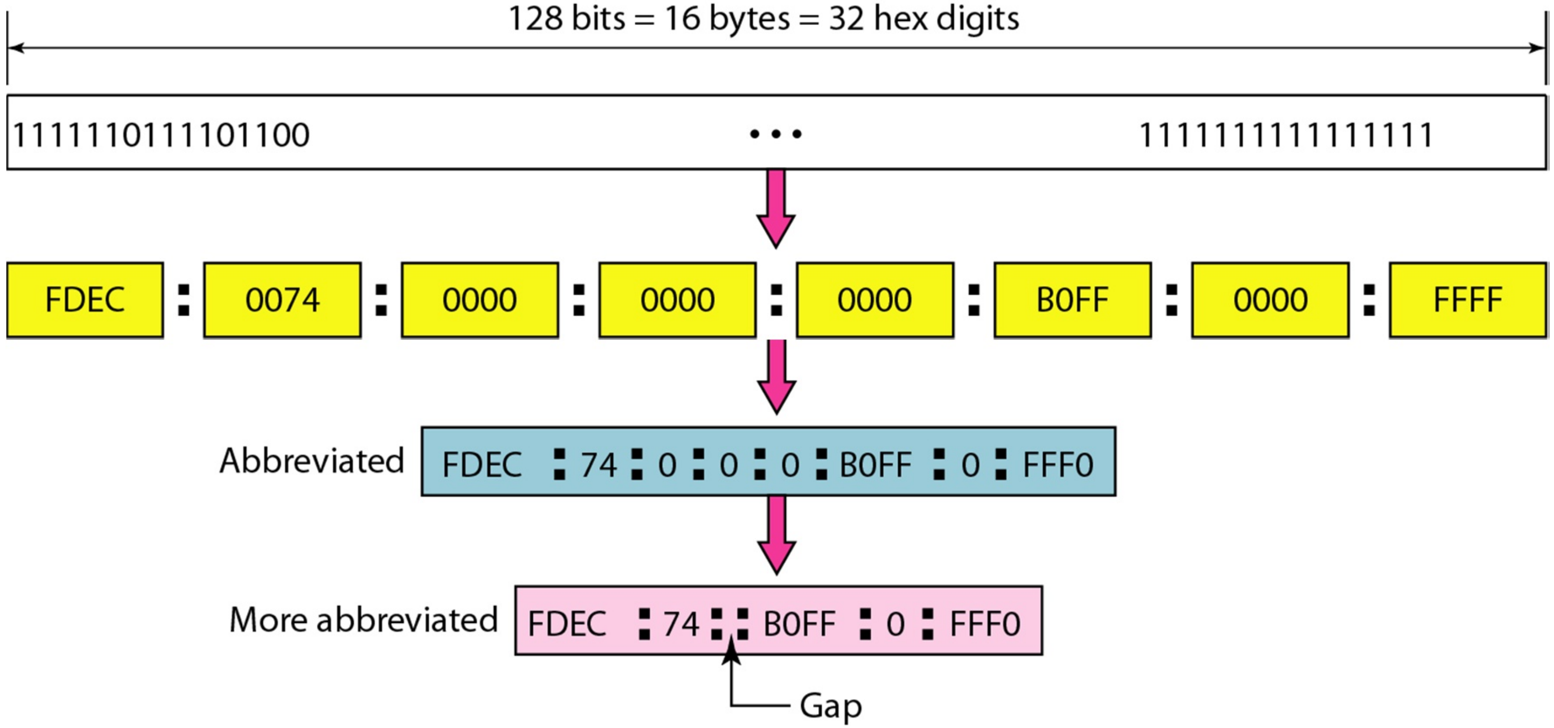
- 128 bits long
- Assigned to interface
- Single interface may have multiple unicast addresses

Three types of addresses:

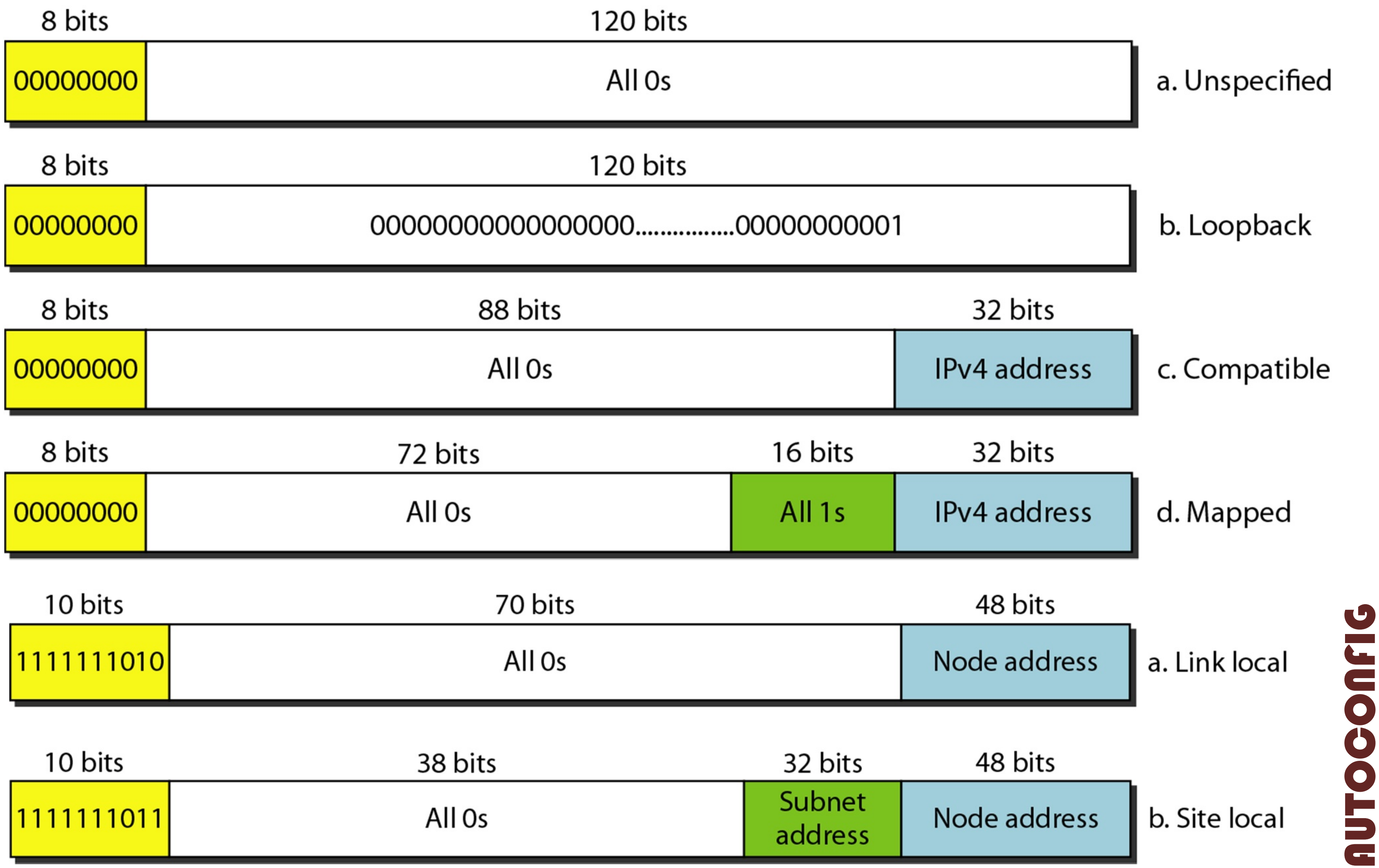
- Unicast - single interface address
- Anycast - one of a set of interface addresses
- Multicast - all of a set of interfaces

IPv6 addresses

- 128 bits = 16 bytes
- $2^{128} = 2^{32} \cdot 2^{96} > 3 \cdot 10^{35}$
- Notations

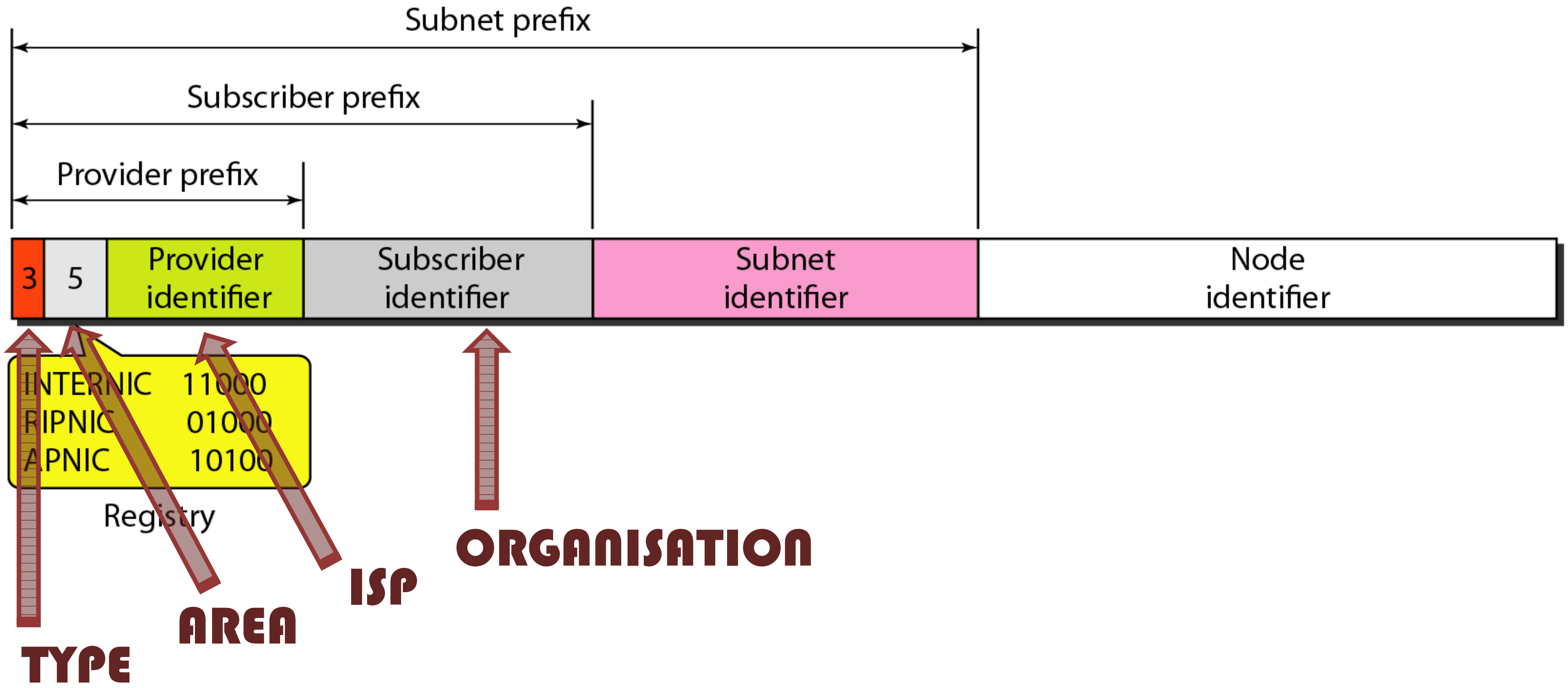


A few special IPv6 addresses



Global unicast addresses

- Note the hierarchy!
- Identify individual computers



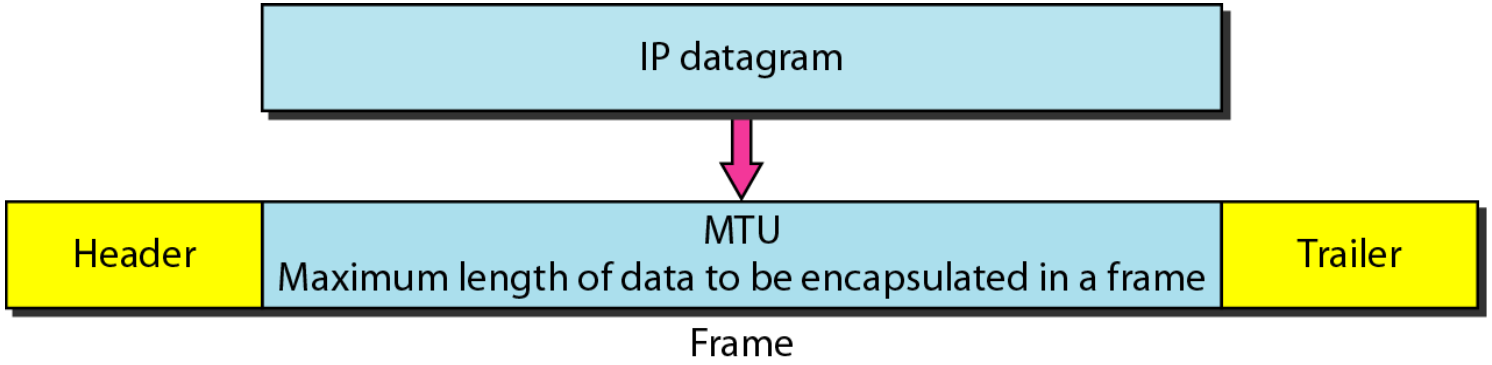
On Fragmentation and Re-assembly

- Protocol exchanges data between two entities
- Lower-level protocols may need to break data up into smaller blocks, called fragmentation
- Reasons for fragmentation:
  - Network only accepts blocks of a certain size
  - More efficient error control and smaller retransmission units
    - Valid argument for framing
  - Fairer access to shared facilities
    - Valid argument for framing
  - Smaller buffers
- Disadvantages:
  - Smaller buffers
  - More interrupts and processing time

Fragmentation

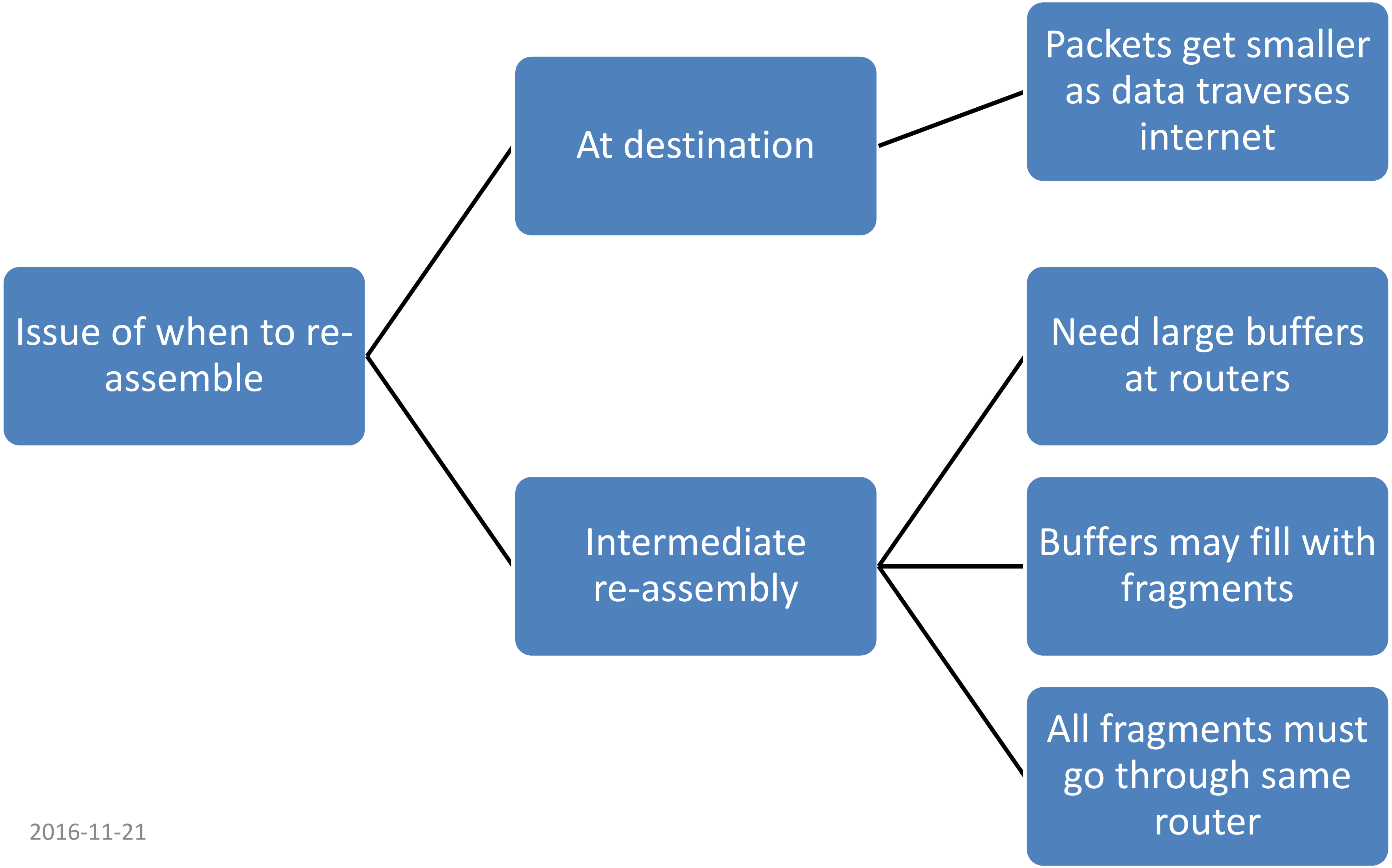
- Needed when IP datagram size > Link layer MTU
- IPv4
  - Performed by the router meeting the problem
- IPv6
  - Performed by the source host only
- Defragmentation by destination host

Maximum datagram size

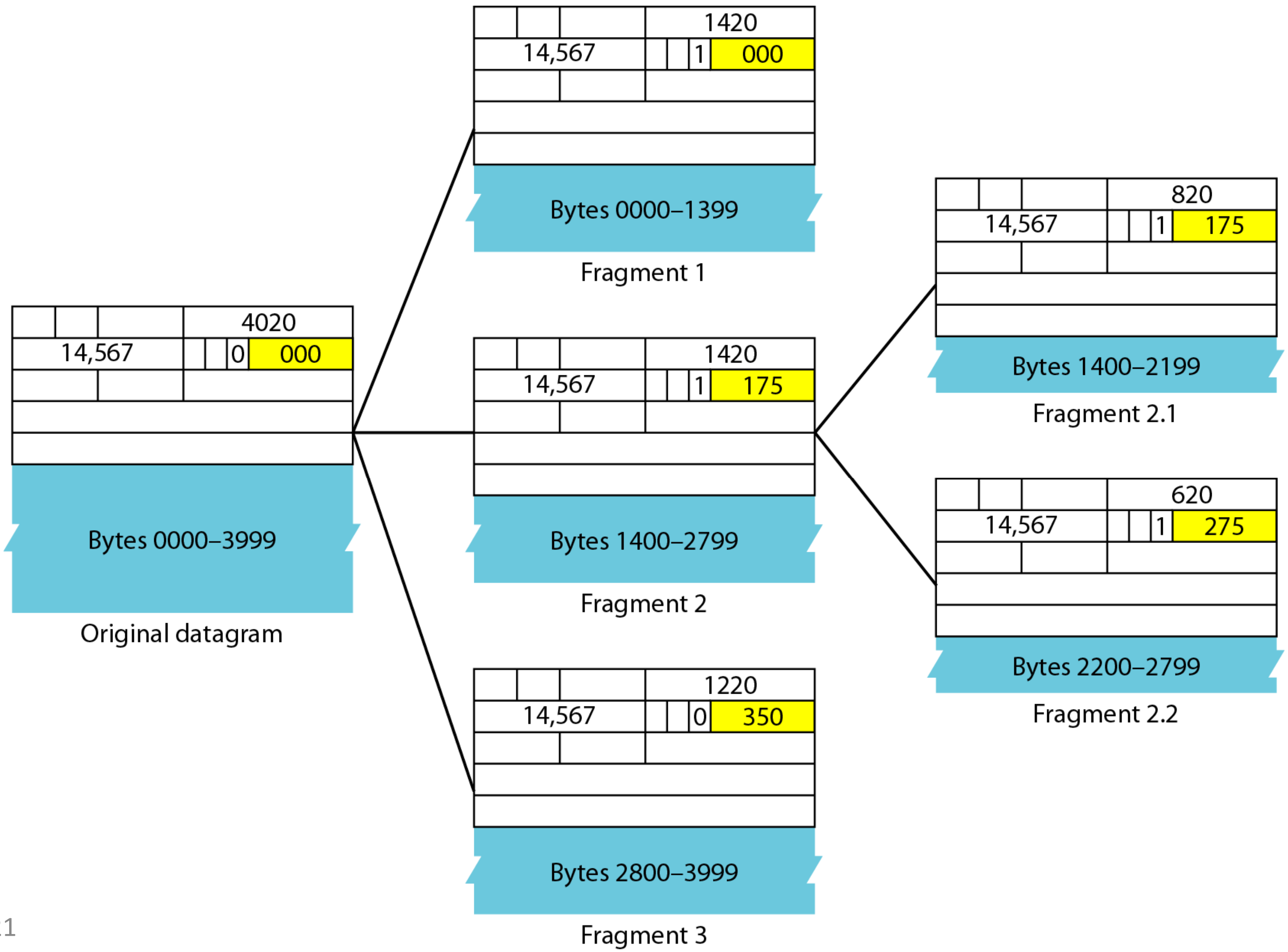


Protocol	MTU
Ethernet (802.3)	1500
Ethernet Jumbo Frames	1501 -- 9198
WLAN (802.11)	7981
PPPoE (Ethernet 802.3)	1492

Fragmentation Re-assembly

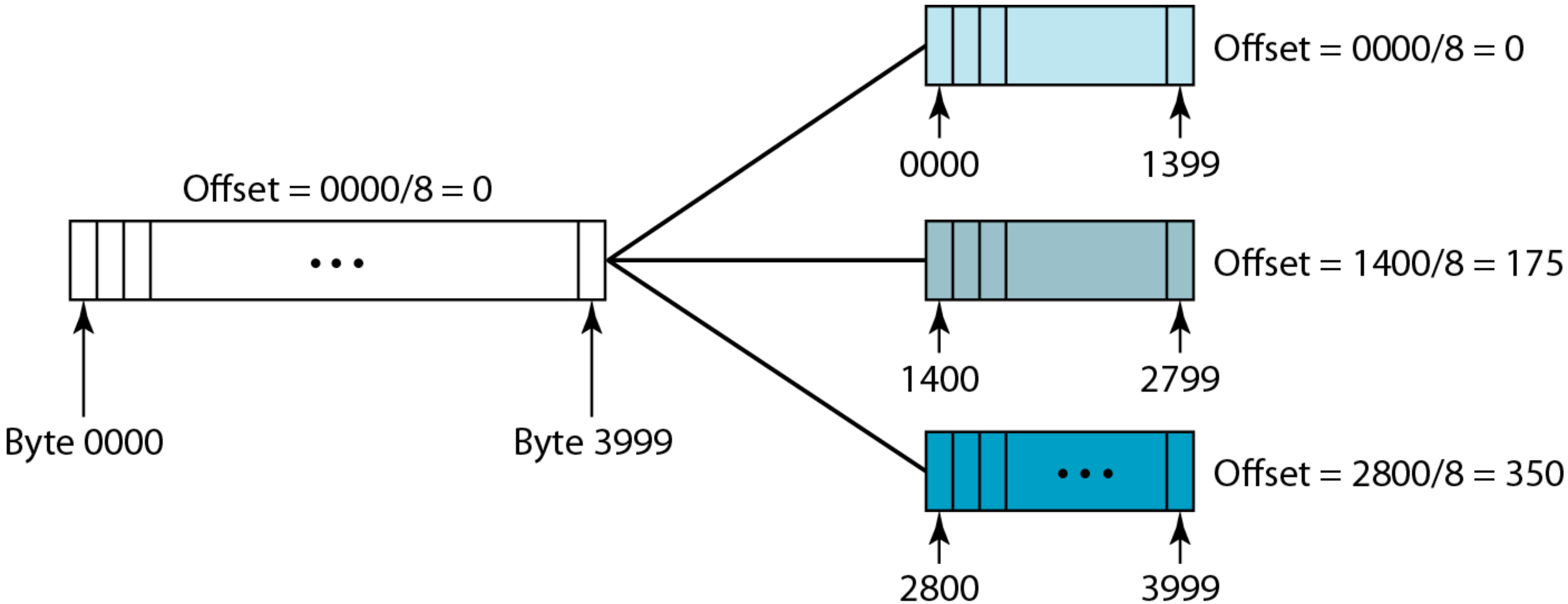


Fragmentation example



Fragmentation offset

- Relative location of fragments
- 13 bits < 16 bits → /8



Path MTU Discovery (PMTUD)

- Works for both IPV6 and IPv4
- Compare with `traceroute`
  - Assume MTU = local LAN MTU
  - Send test packet with Don’t Fragment flag set
  - If MTU < IP packet size node return ICMP error msg containing its MTU
    - ICMPv4: *Fragmentation Needed*
    - ICMPv6 : *Packet Too Big*
  - Reduce IP packet size and try again.

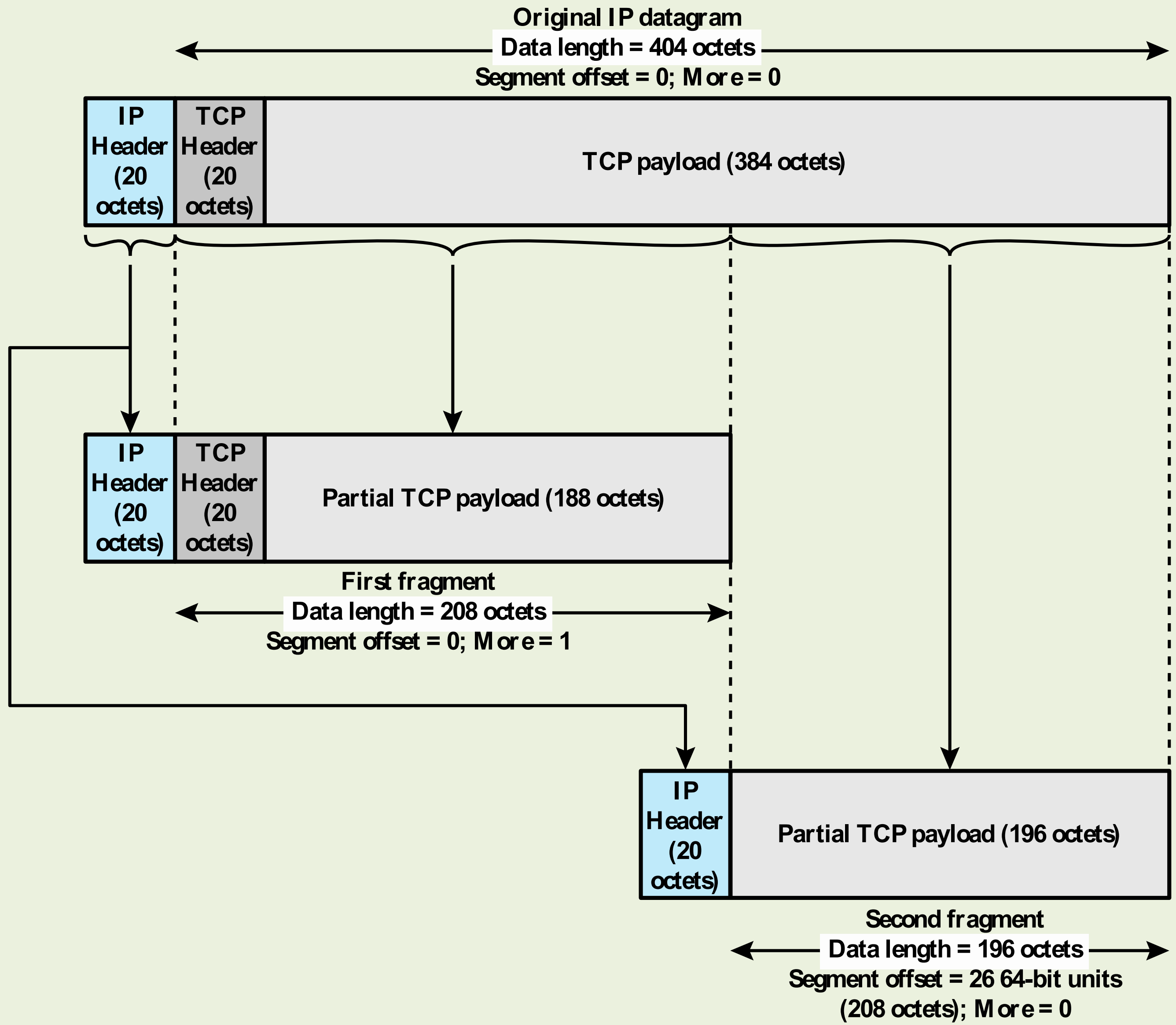
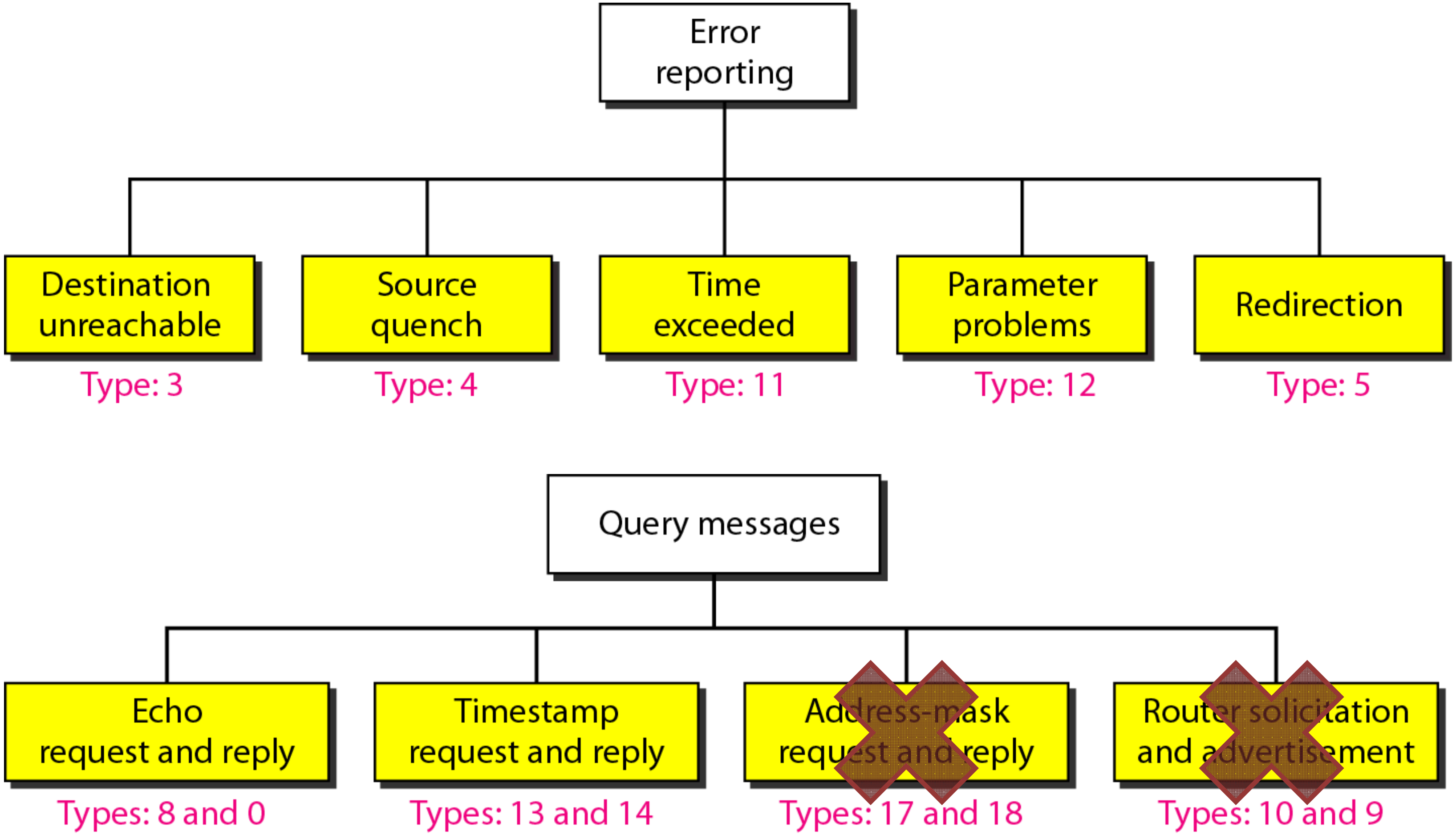


Figure 14.4 Fragmentation Example

Internet Control Message Protocol (ICMP)

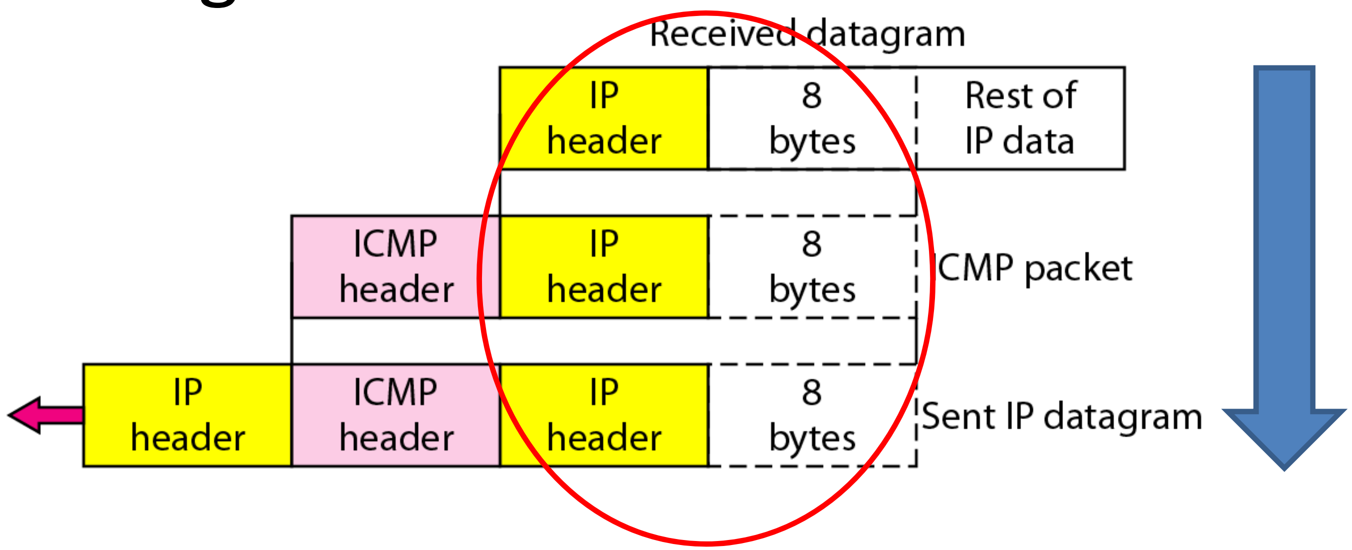
- RFC 792
- Provides a means for transferring messages from routers and other hosts to a host
- Provides feedback about problems
    - Datagram cannot reach its destination
    - Router does not have buffer capacity to forward
    - Router can send traffic on a shorter route
- Encapsulated in IP datagram
    - – Hence not reliable

ICMPv4 message types

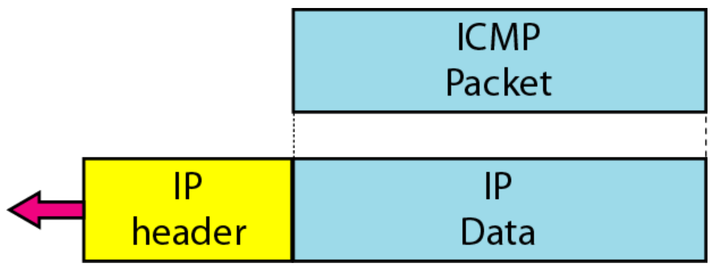


ICMP message formats

- Error reporting



- Query messages



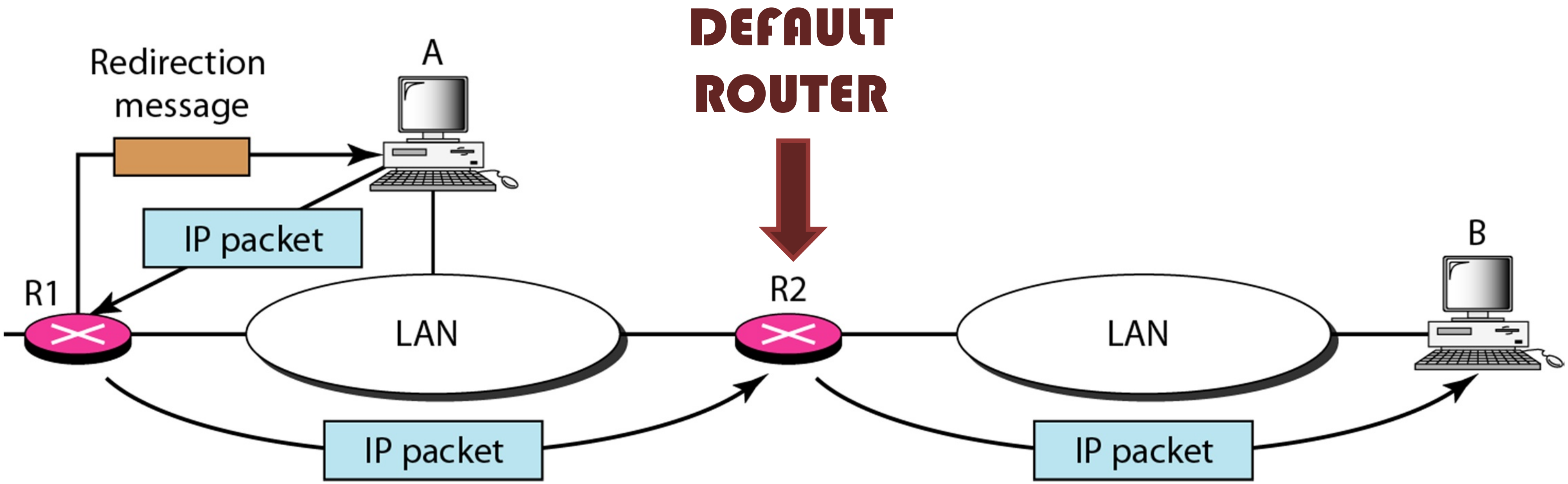
Echo request and reply (query type)

- Is my destination alive?

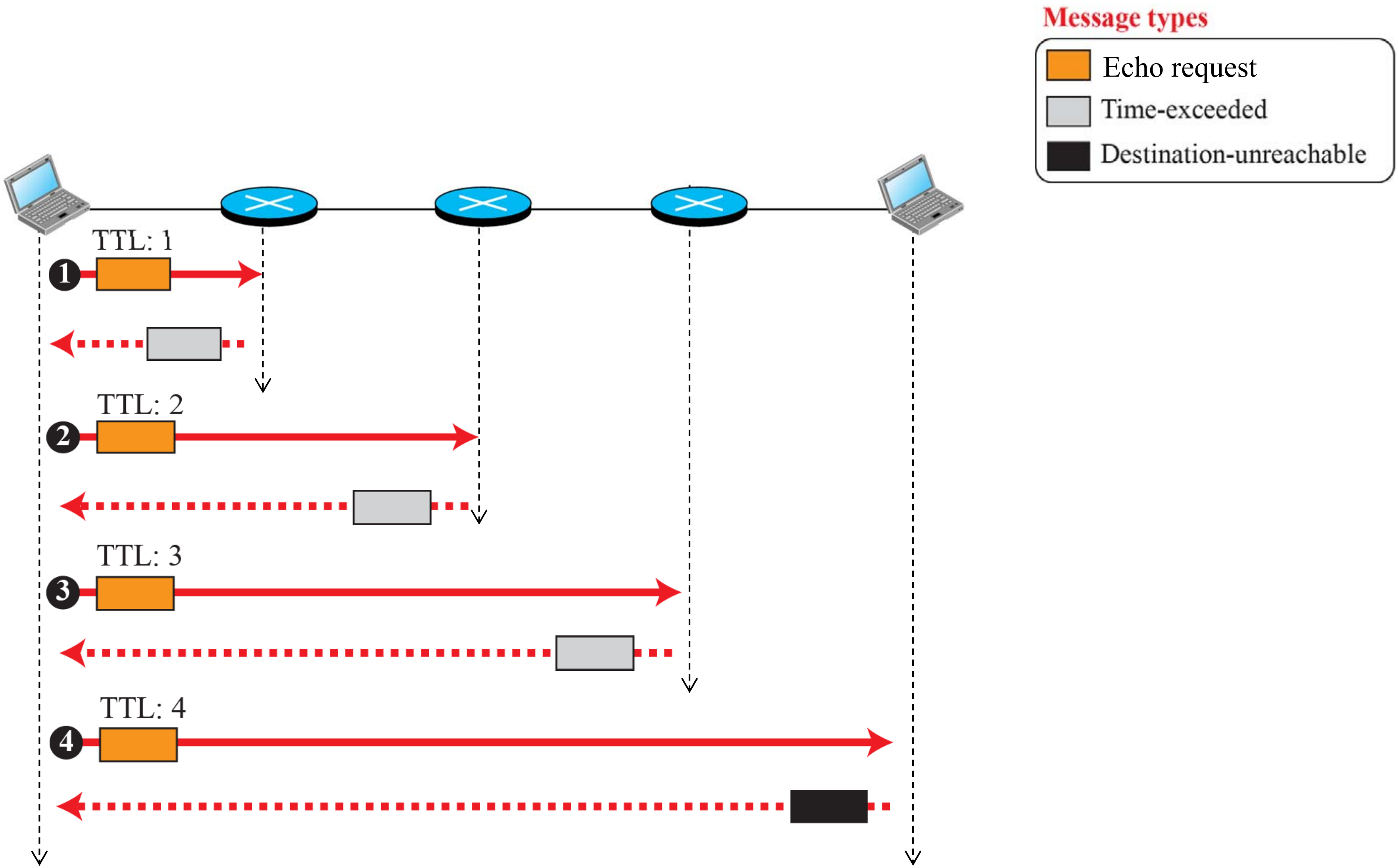
- Network diagnostics
  - IP layer
- Debugging tools
  - Ping
  - Traceroute

Redirection (error reporting type)

- Routing update for hosts
  - More efficient when too many hosts



Traceroute



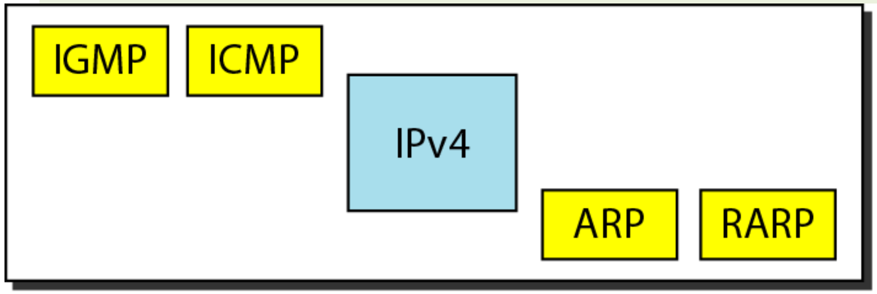
Message types
Echo request
Time-exceeded
Destination-unreachable
TTL: 1
1
TTL: 2
2
TTL: 3
3
TTL: 4
4

ICMPv6

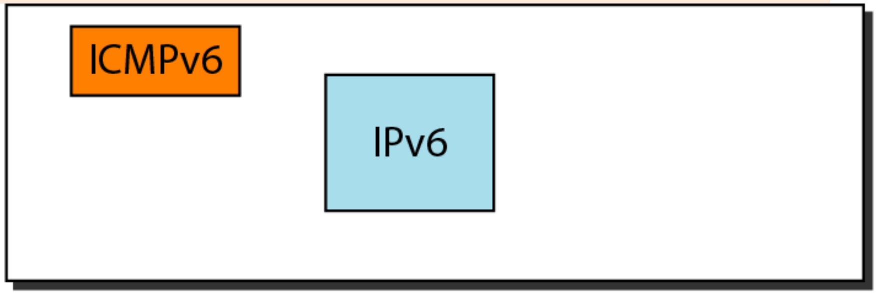
- Includes ”IPv4 IGMP”
  - Group membership messages
    - Multicast Listener Delivery protocol (MLD)
- Includes ”IPv4 ARP”
  - Part of Neighbor Discovery Protocol (NDP)

Changes to ICMP

ICMPv4	*ICMPv6*
• Some unused functions	• Same principle • Some new functions • Convergence • Suits IPv6 better



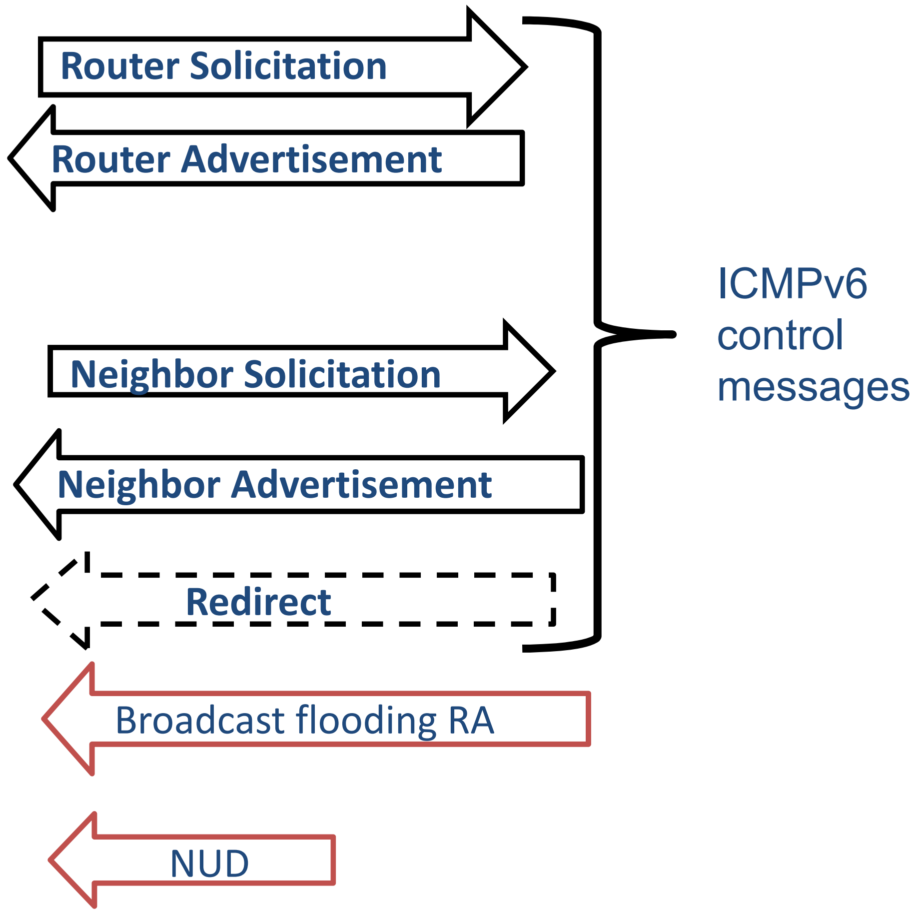
Network layer in version 4



Network layer in version 6

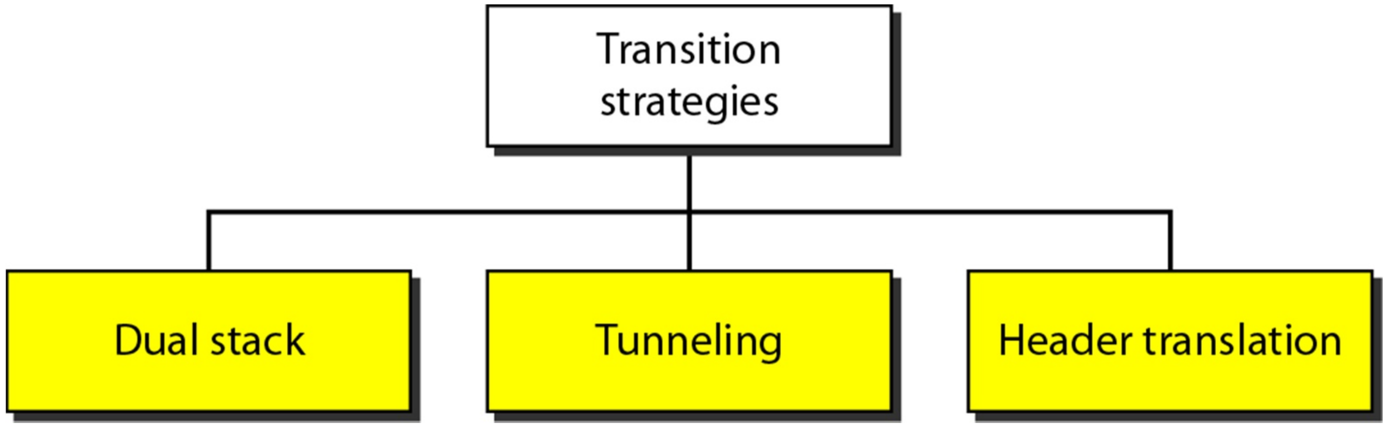
ICMPv6 ND and AAC

1. Router Discovery
2. Address Configuration Mechanism (RFC 4862)
3. Address Resolution
4. Duplicate Address Detection
5. Updating a change of MAC address to the network
6. Neighbor Unreachability



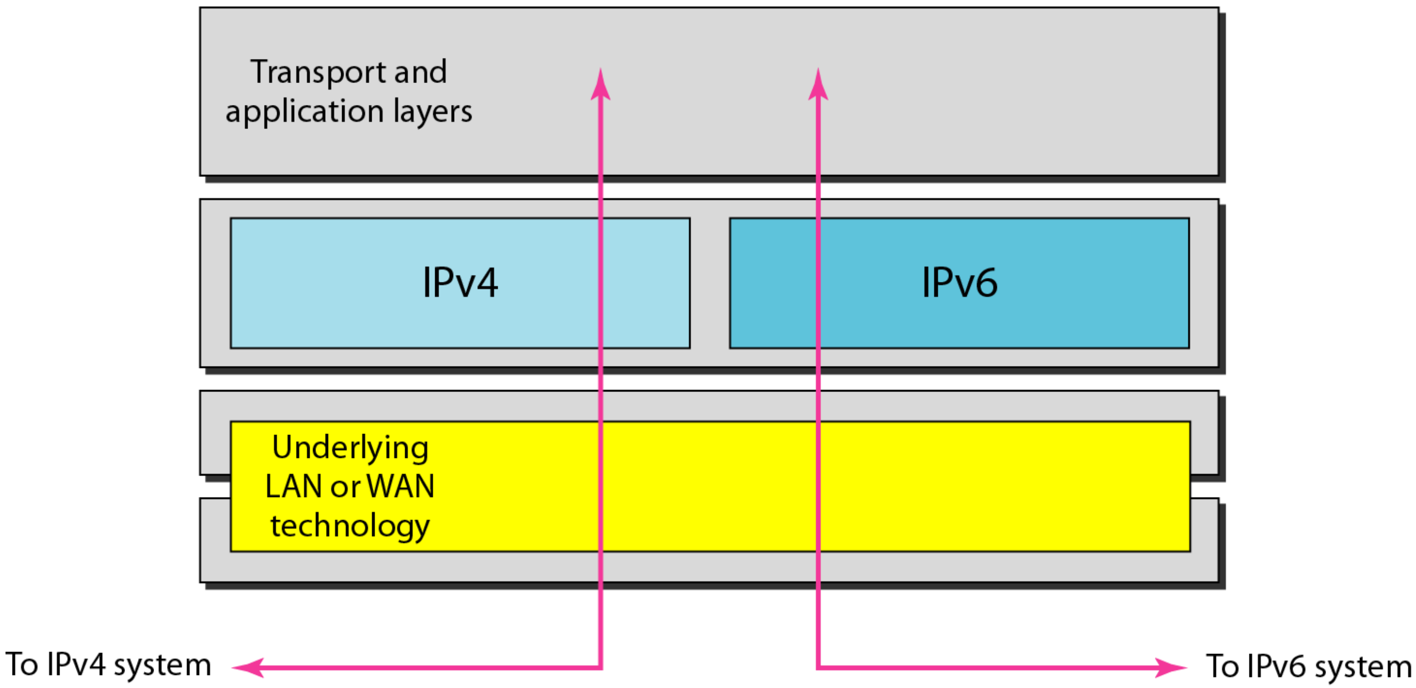
Transition: IPv4 → IPv6

- Cannot happen overnight
  - Too many independent systems
  - Economic cost
  - IPv4 address space lasted longer than expected
- Coexisence needed



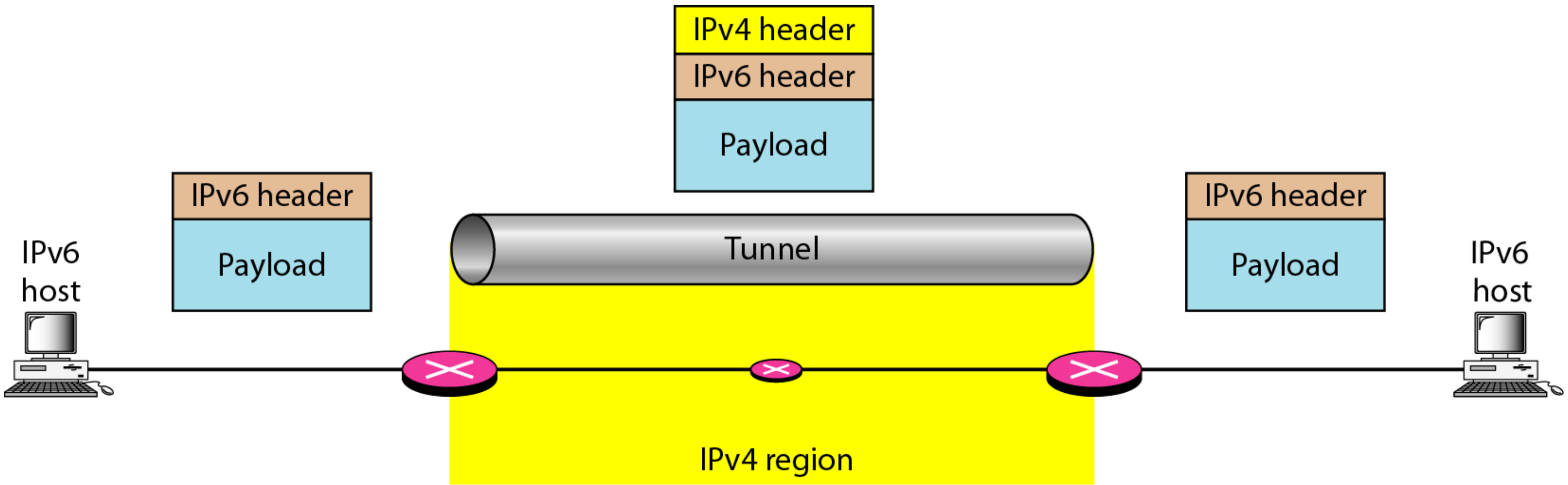
Transition: (1) Dual stack

- Decision based on destination IP



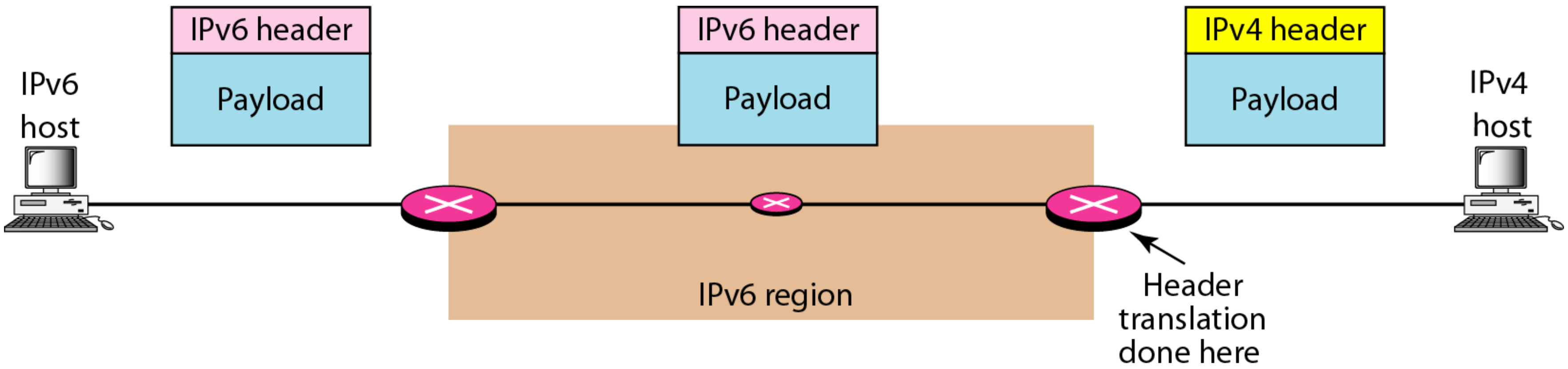
Transition: (2) Tunneling

- A few IPv6 routers



Transition: (3) Header translation

- A few IPv4 routers



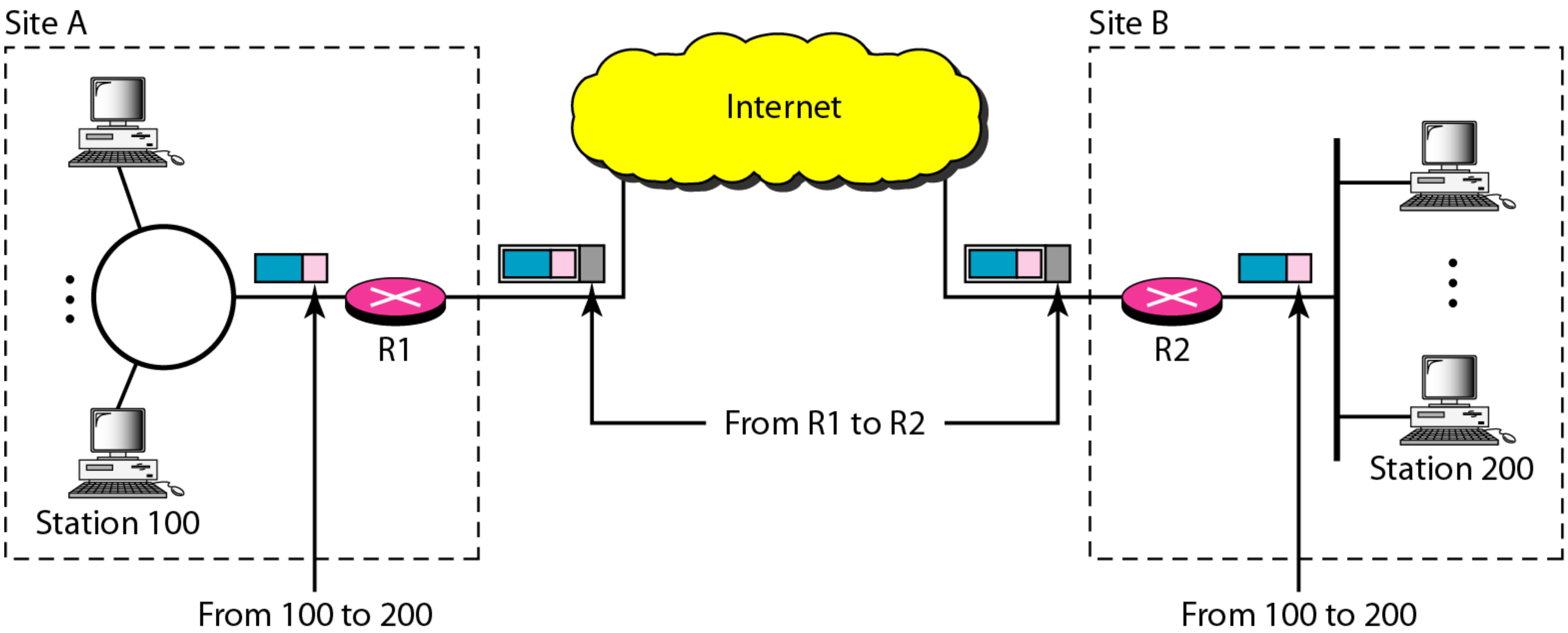
Virtual Private Network (VPN)

- Set of computers interconnected using an unsecure network
    - e.g. linking corporate LANs over Internet
- Using encryption and special protocols to provide security
    - Eavesdropping
    - Entry point for unauthorized users

- Proprietary solutions are problematical
    - Development of IPSec standard

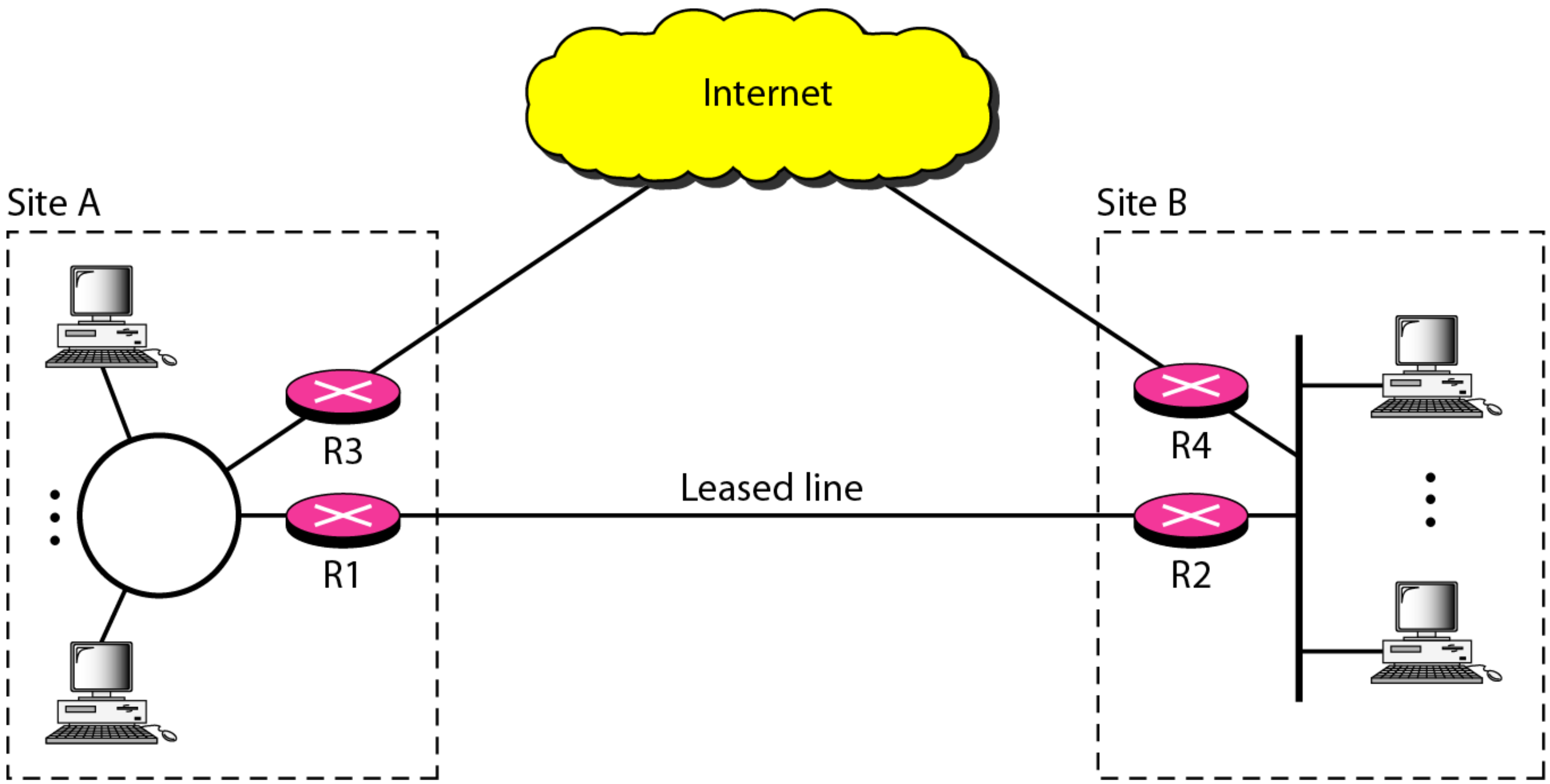
An example VPN

- IPSec between routers



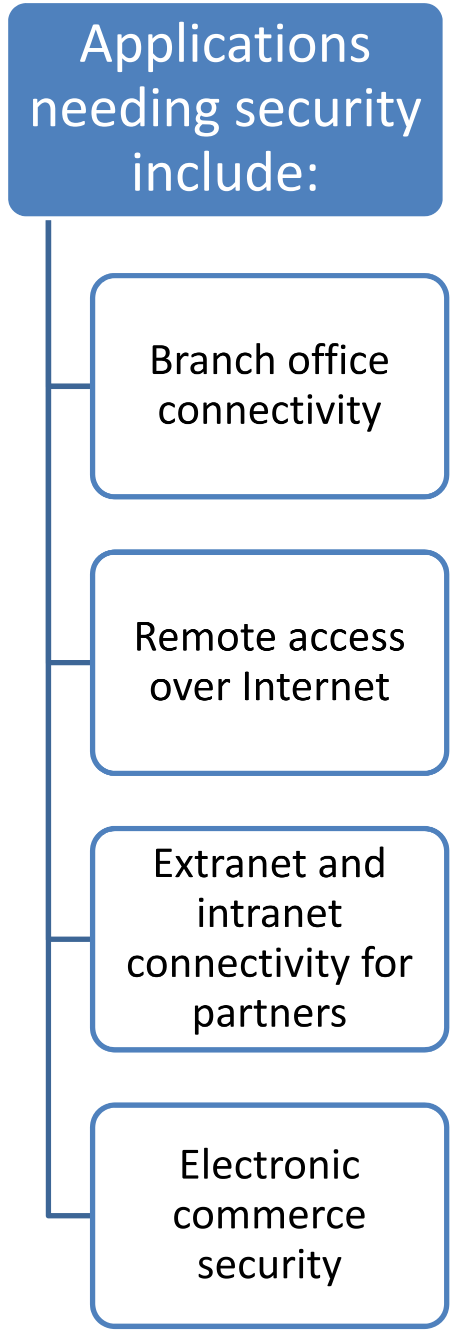
Virtual Private Network (VPN)

- Overlay network
- Alternative to a real private network



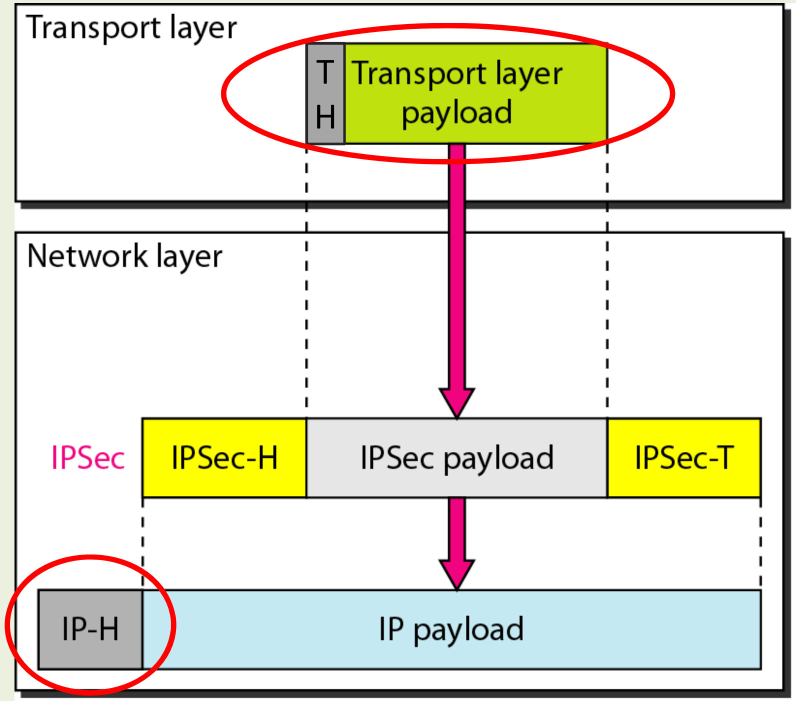
IPsec

- RFC 1636 (1994) identified security need
- Encryption and authentication necessary security **features in IPv6**
- Designed **also for use with current IPv4**



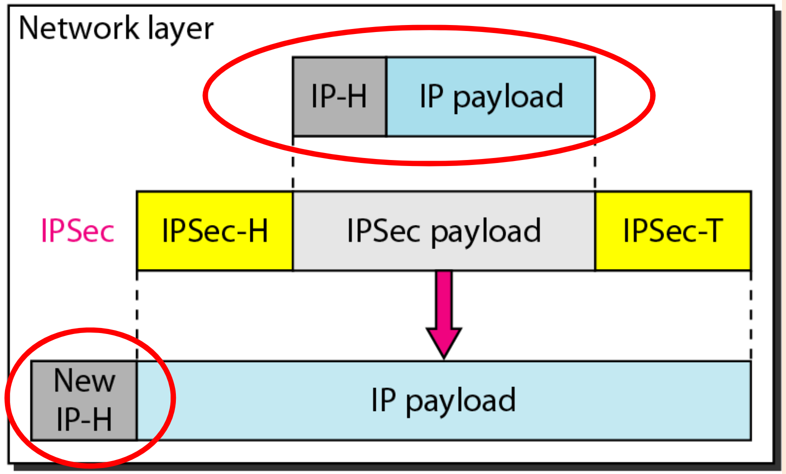
IPSec

Transport mode



a. Transport mode

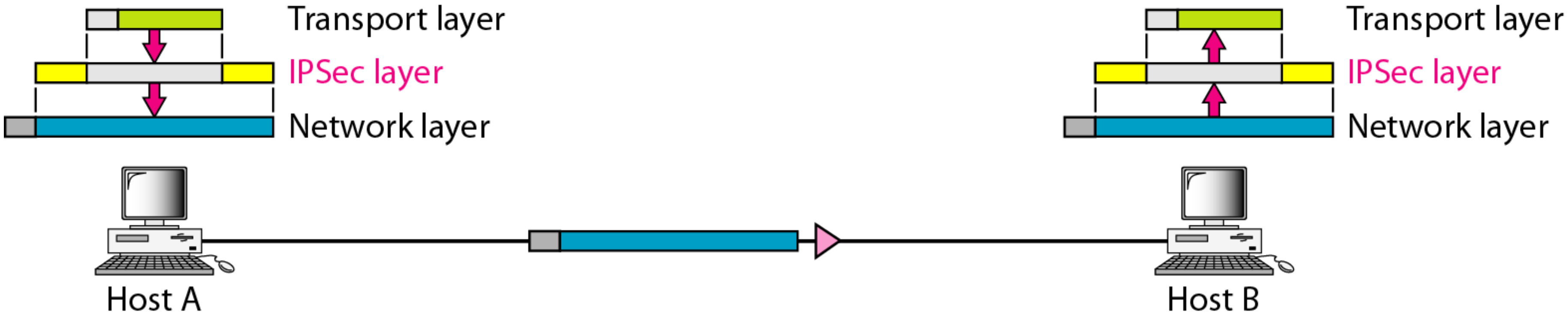
Tunnel mode



b. Tunnel mode

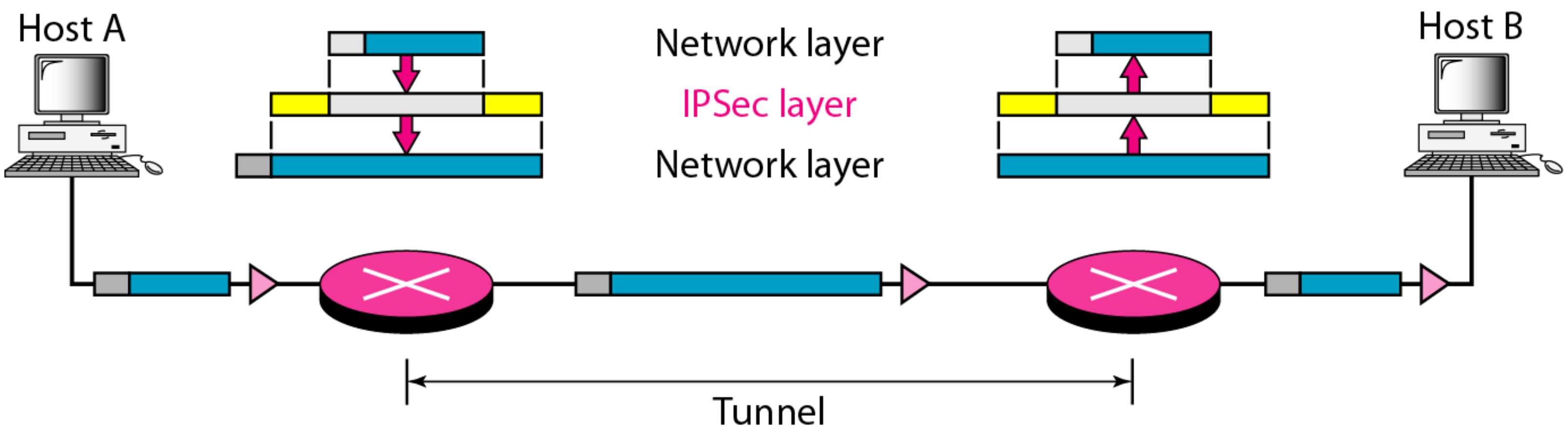
Transport mode in action

- Data protected
- Headers unprotected
  - Addresses fully visible

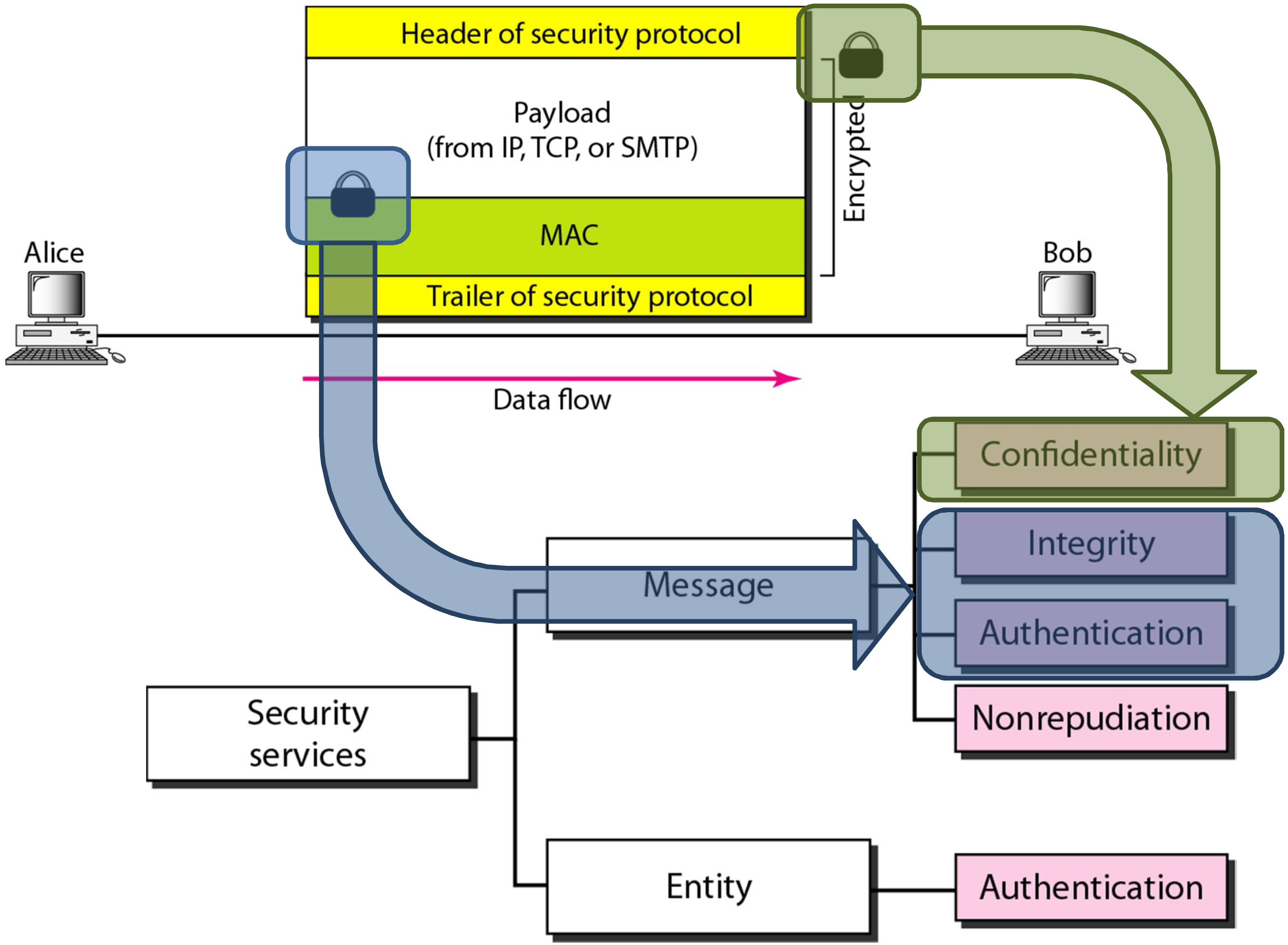


Tunnel mode in action

- Not used between hosts
- Entire packet protected
  - New header inside tunnel



Internet security



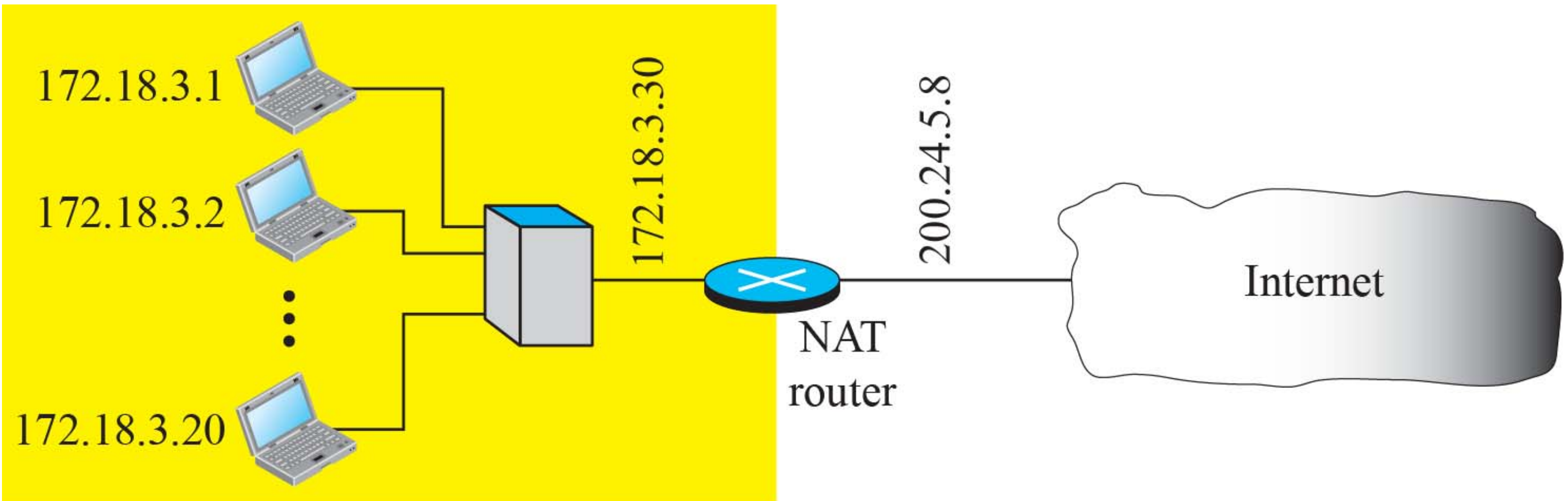
VPN alternatives (bonus material)

- PPTP (Point-to-Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol)
- SSTP (Secure Socket Tunneling Protocol)
- OpenVPN

- See Wikipedia for information

NAT - Network Address Translation

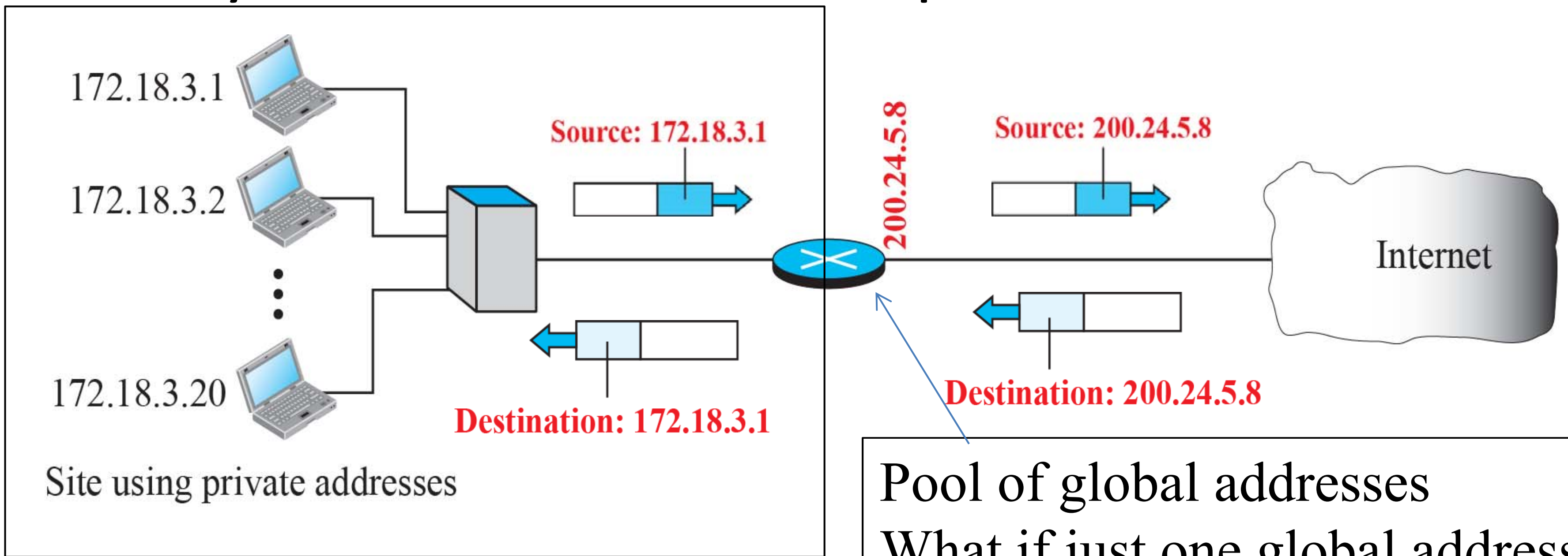
- Sharing of routable addresses (scarse resource)
- Adds some security …



Site using private addresses

NAT (network address only)

- Change source address on outgoing packets
- Add address pair to active translations table
  - Inside source + outside destination
- Only one internal address per destination



Pool of global addresses
What if just one global address?

NAPT, NAT extended

- Add transport layer port

Private Address	Private Port	External Address	External Port	Transport Protocol
172.18.3.1	1400	200.24.5.8	1000	TCP
172.18.3.3	2345	200.24.5.8	1001	TCP
172.18.3.1	80	200.24.5.8	8080	TCP

- Normally initiated from inside
- Port forwarding: Setup static entry in table