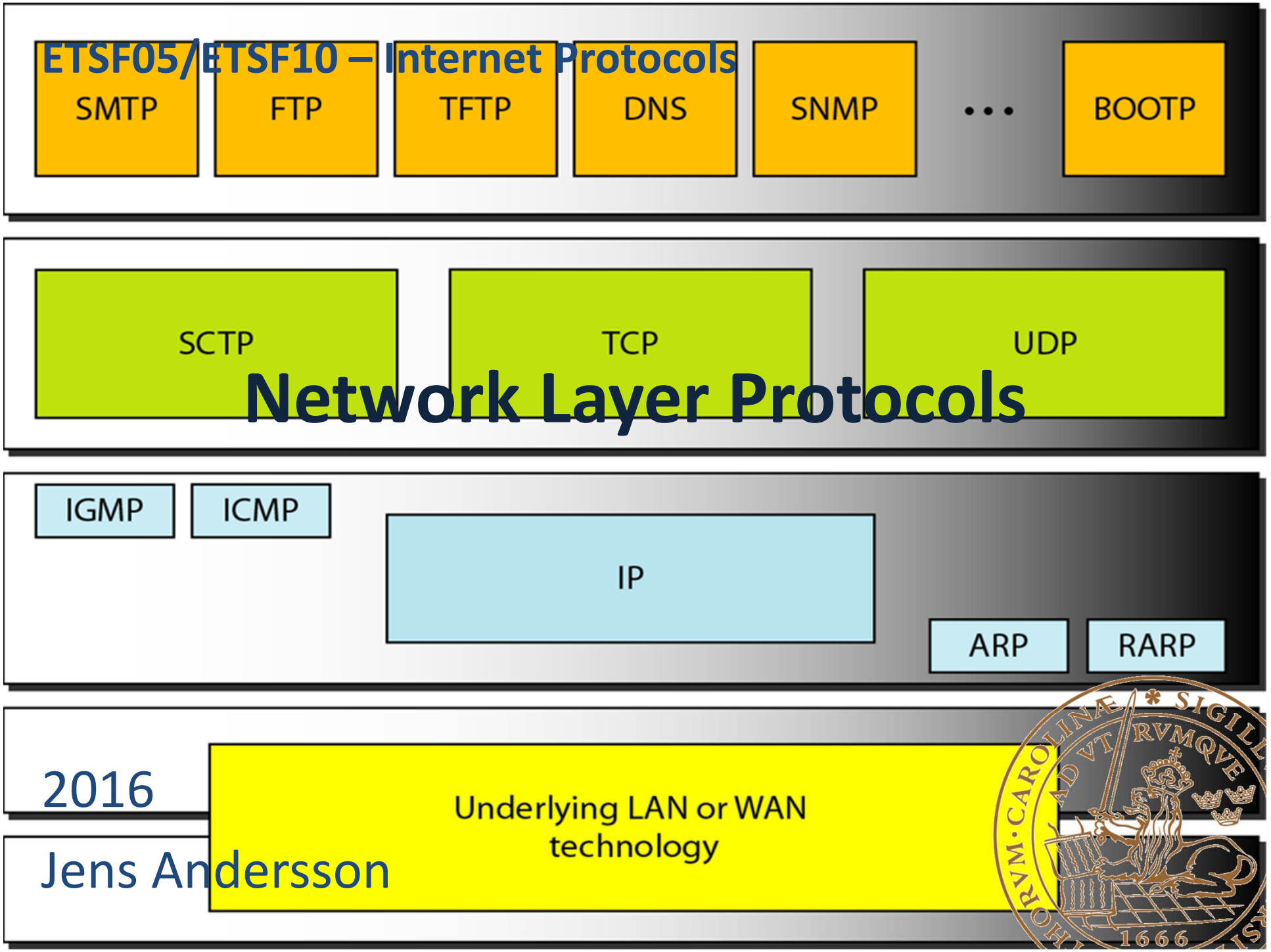
“The requirements for a future all-digital-data distributed network which provides common user service for a wide range of users having different requirements is considered. The use of a standard format message block permits building relatively simple switching mechanisms using an adaptive store-and-forward routing policy to handle all forms of digital data including "real-time" voice. This network rapidly responds to changes in network status.”

—On Distributed Communications,
Rand Report RM-3420-PR,
Paul Baran, August 1964

ETSF05/ETSF10 – Internet Protocols



2016

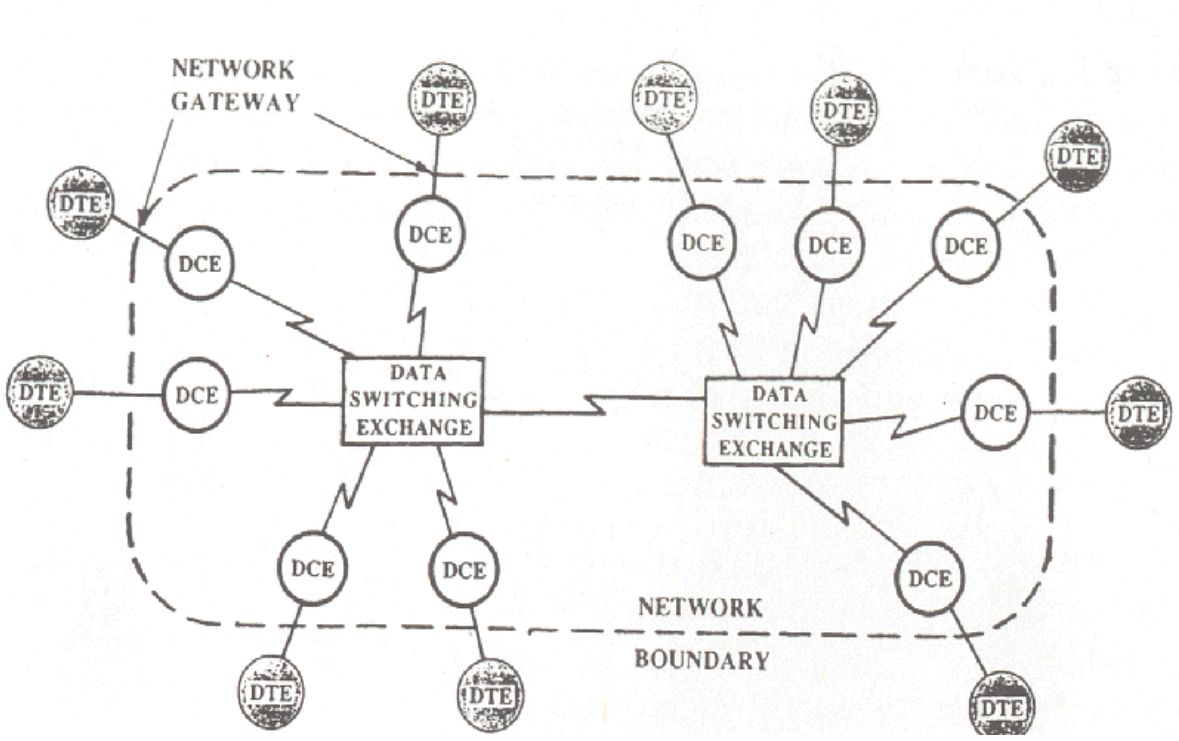
Jens Andersson

Agenda

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

Packet switched networks

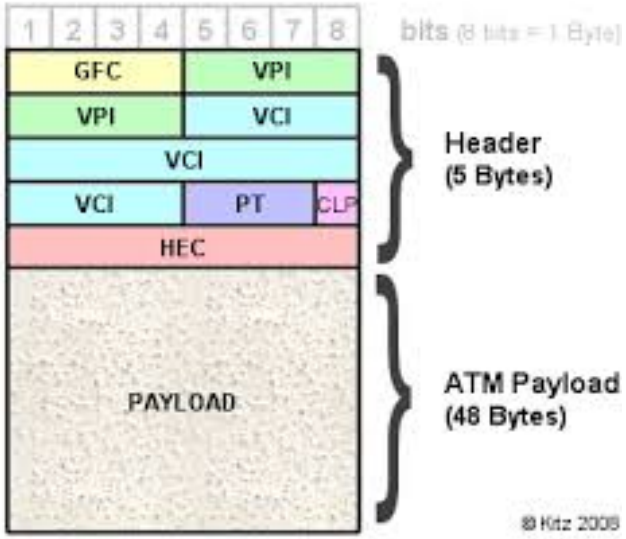
•Several people proposed the idea of packet switched networks in the early 1960s.

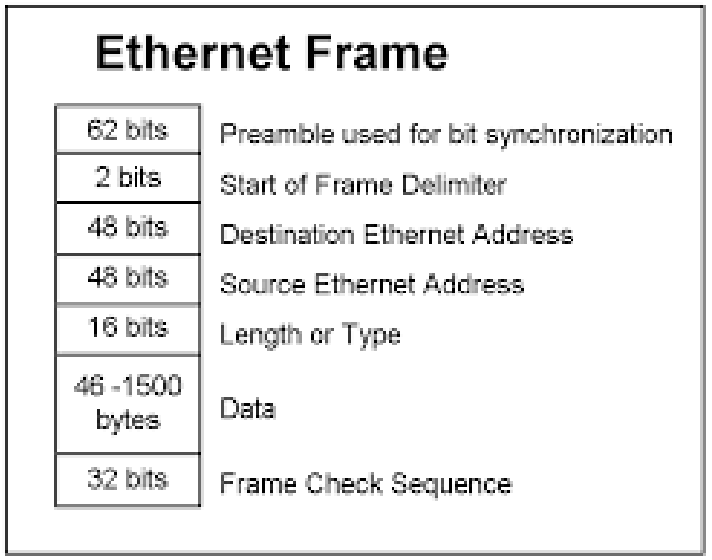


Source: http://www.samhassan.com

Example of Two Link Layer Protocols

ATM cell

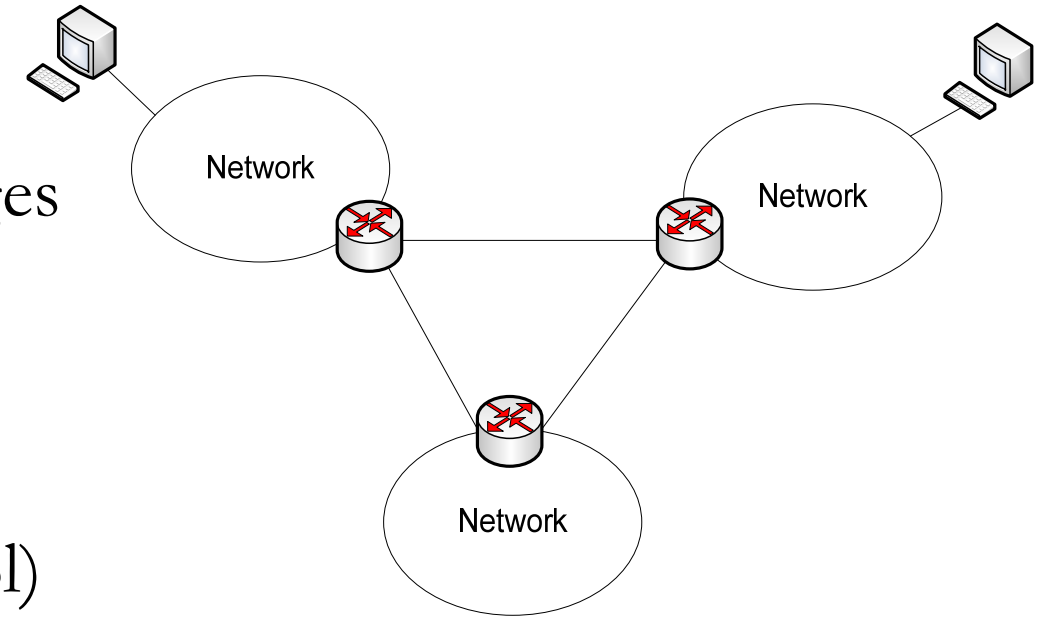




No network id in neither protocol
Different addressing methods
Different frame formats

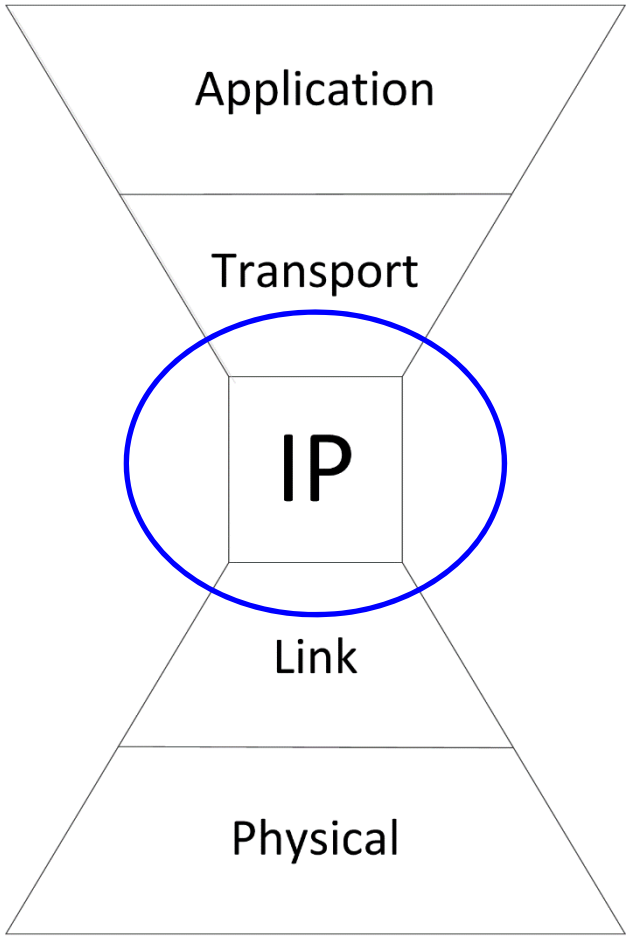
Basic idea of Kahn and Cerf's internetworking

- 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



Connectionless Internetworking

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

Communication Network
A facility that provides a data transfer service among devices attached to the network.

Internet
A collection of communication networks interconnected by bridges and/or routers.

Intranet
An internet used by a single organization that provides the key Internet applications, especially the World Wide Web. An intranet operates within the organization for internal purposes and can exist as an isolated, self-contained internet, or may have links to the Internet.

Subnetwork
Refers to a constituent network of an internet. This avoids ambiguity because the entire internet, from a user's point of view, is a single network.

End System (ES)
A device attached to one of the networks of an internet that is used to support end-user applications or services.

Intermediate System (IS)
A device used to connect two networks and permit communication between end systems attached to different networks.

Bridge
An IS used to connect two LANs that use similar LAN protocols. The bridge acts as an address filter, picking up packets from one LAN that are intended for a destination on another LAN and passing those packets on. The bridge does not modify the contents of the packets and does not add anything to the packet. The bridge operates at layer 2 of the OSI model.

Router
An IS used to connect two networks that may or may not be similar. The router employs an internet protocol present in each router and each end system of the network. The router operates at layer 3 of the OSI model.

Table 14.1

Internetworking Terms (use as reference)

(Table is on page 453 in the textbook)

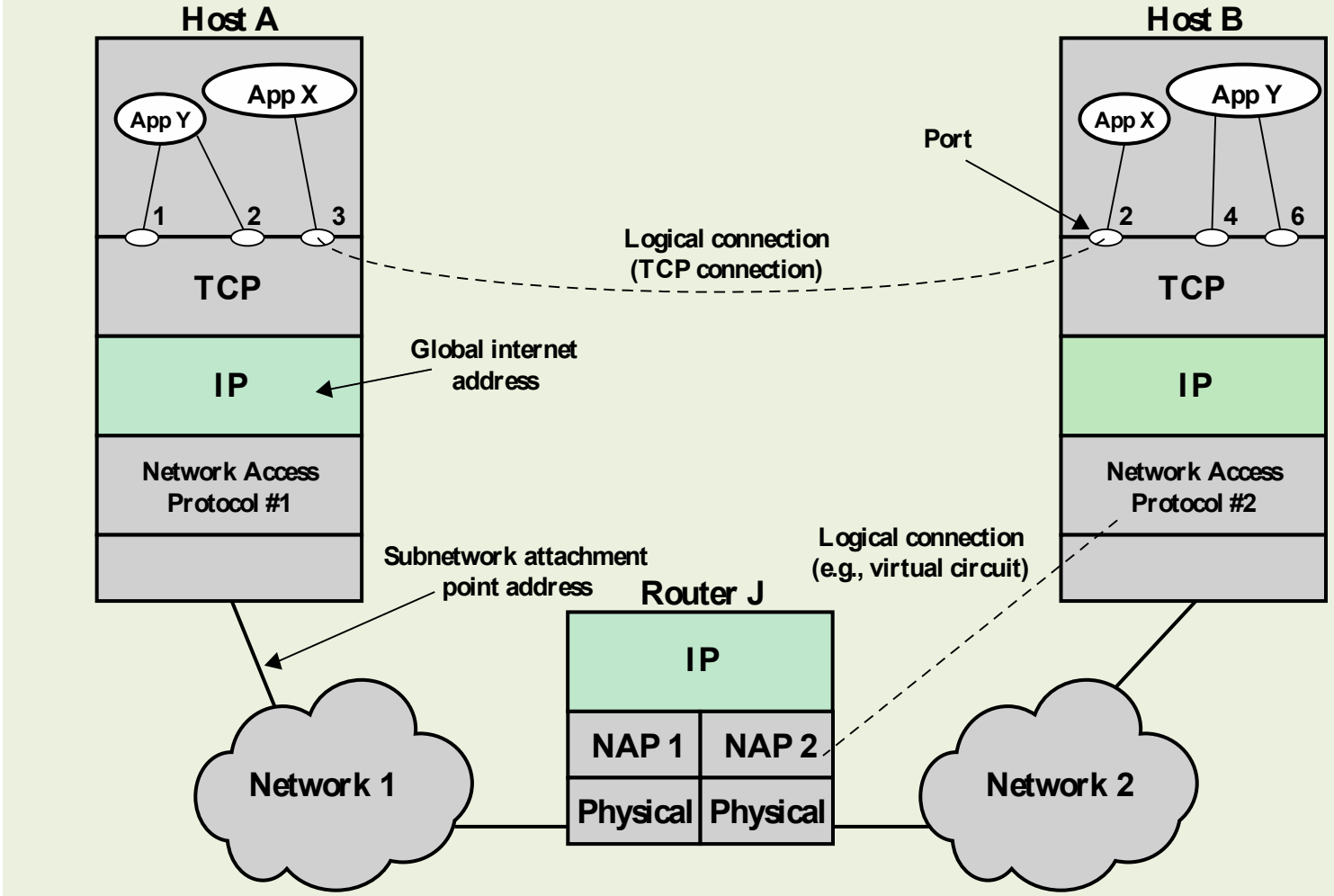


Figure 14.1 TCP/IP Concepts

Internet Protocol (IP) v4

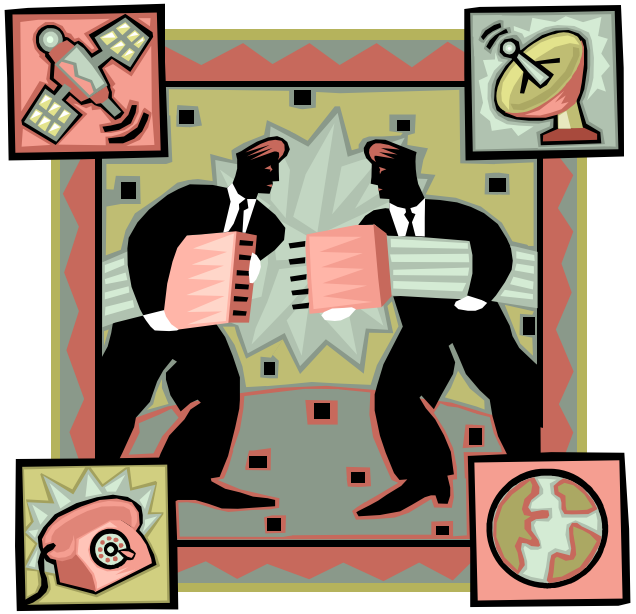
- Defined in RFC 791
- Part of TCP/IP suite
- Two specifications:

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 Parameters (refresher)

- Source and destination addresses
- Protocol
- Type of Service
- Identification
- Don’t fragment indicator
- Time to live
- Data length
- Option data
- User data

IPv4 Options

Security

Route recording

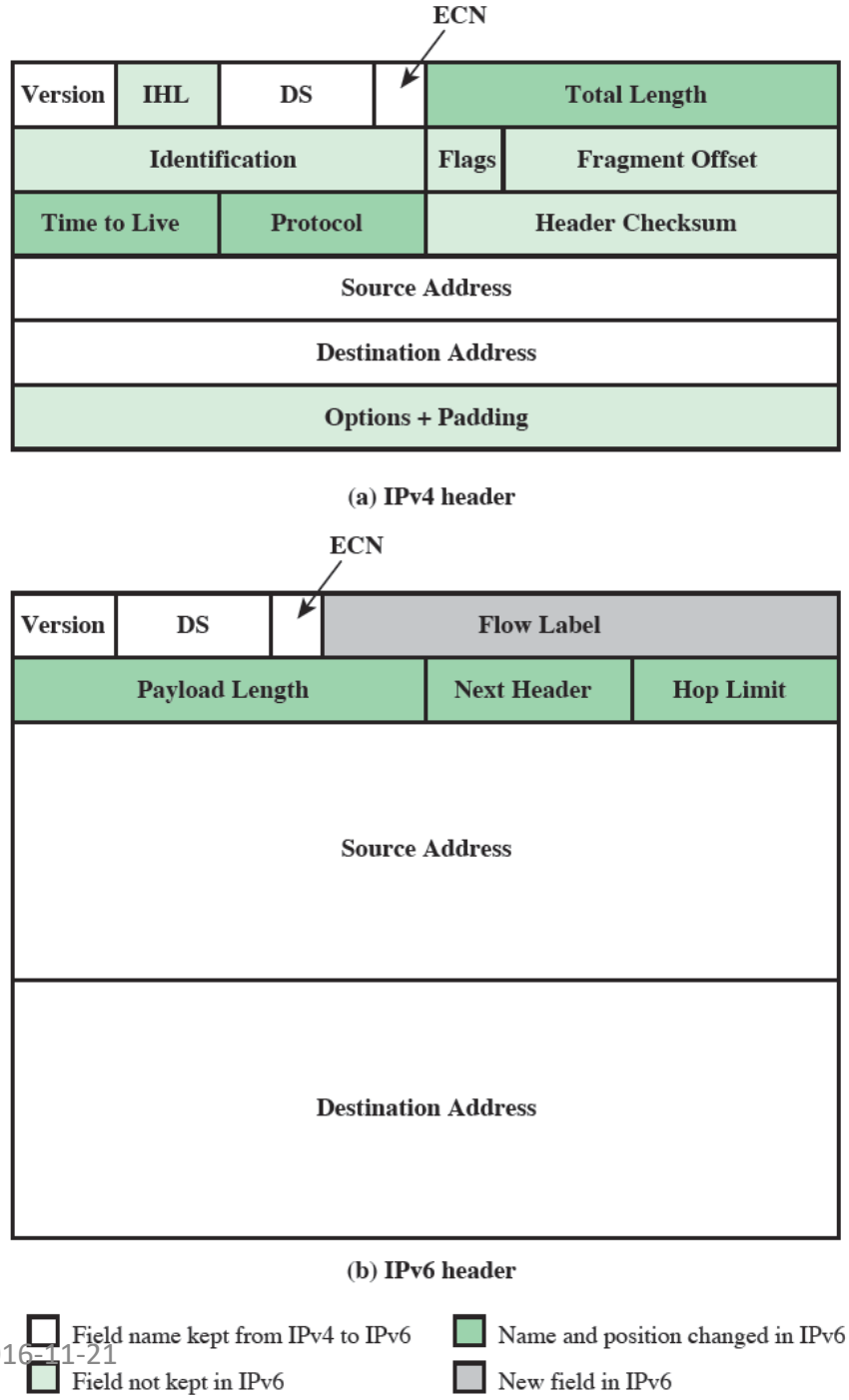
Source routing

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)

Internet of Things

IPv6 RFCs (use as reference)

- RFC 1752 - Recommendations for the IP Next Generation Protocol
  - Requirements
  - PDU formats
  - Addressing, routing security issues
- RFC 2460 - overall specification
- RFC 4291 - addressing structure
- RFC 4861 Neighbour Discovery

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

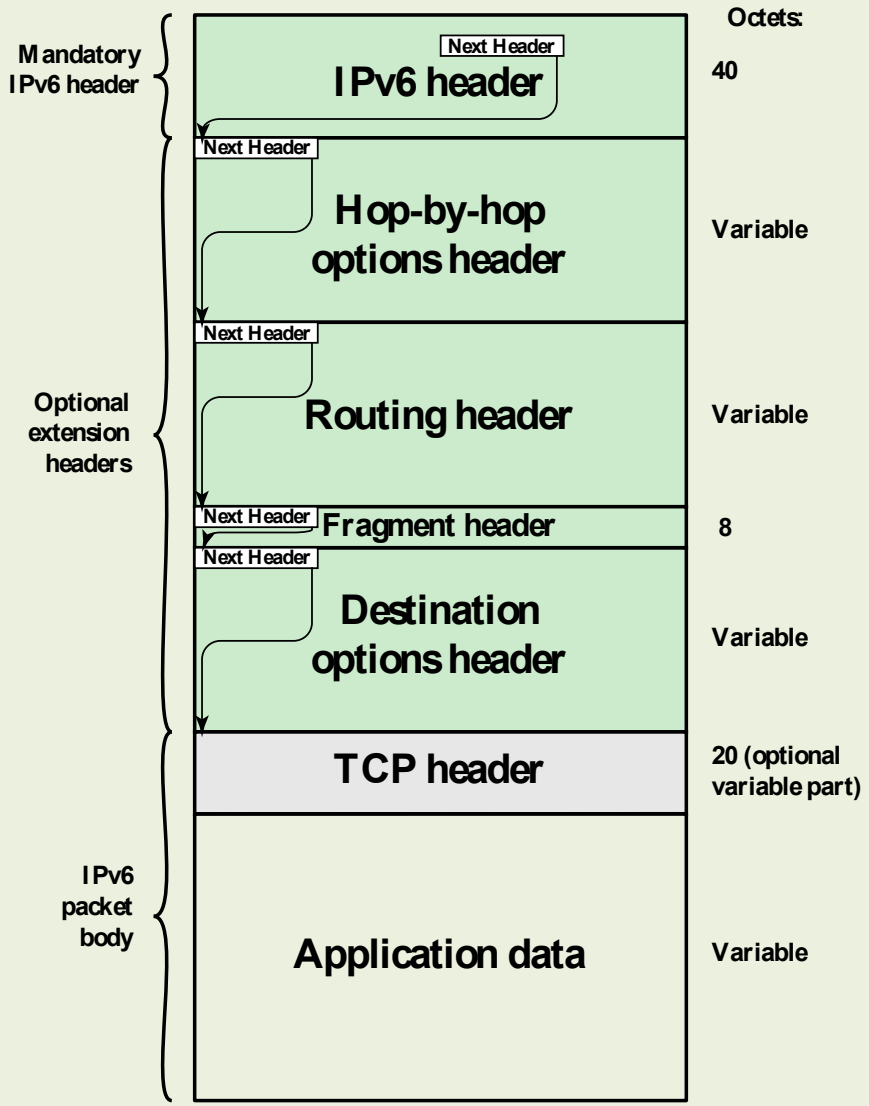
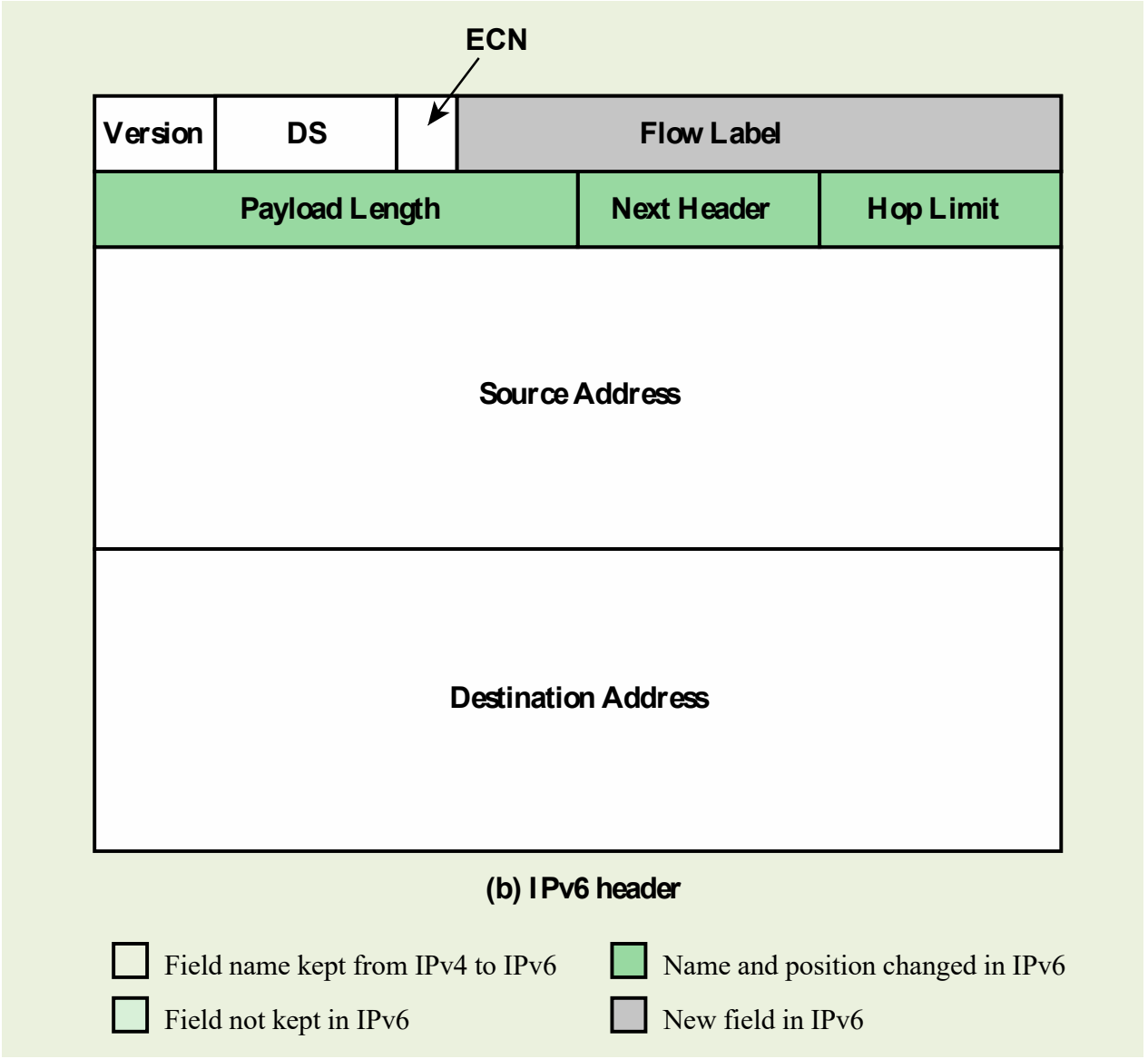


Figure 14.9 IPv6 Packet with Extension Headers (containing a TCP Segment)

IPv6 Header and Option Fields

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


ECN
Version
DS
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address
(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 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

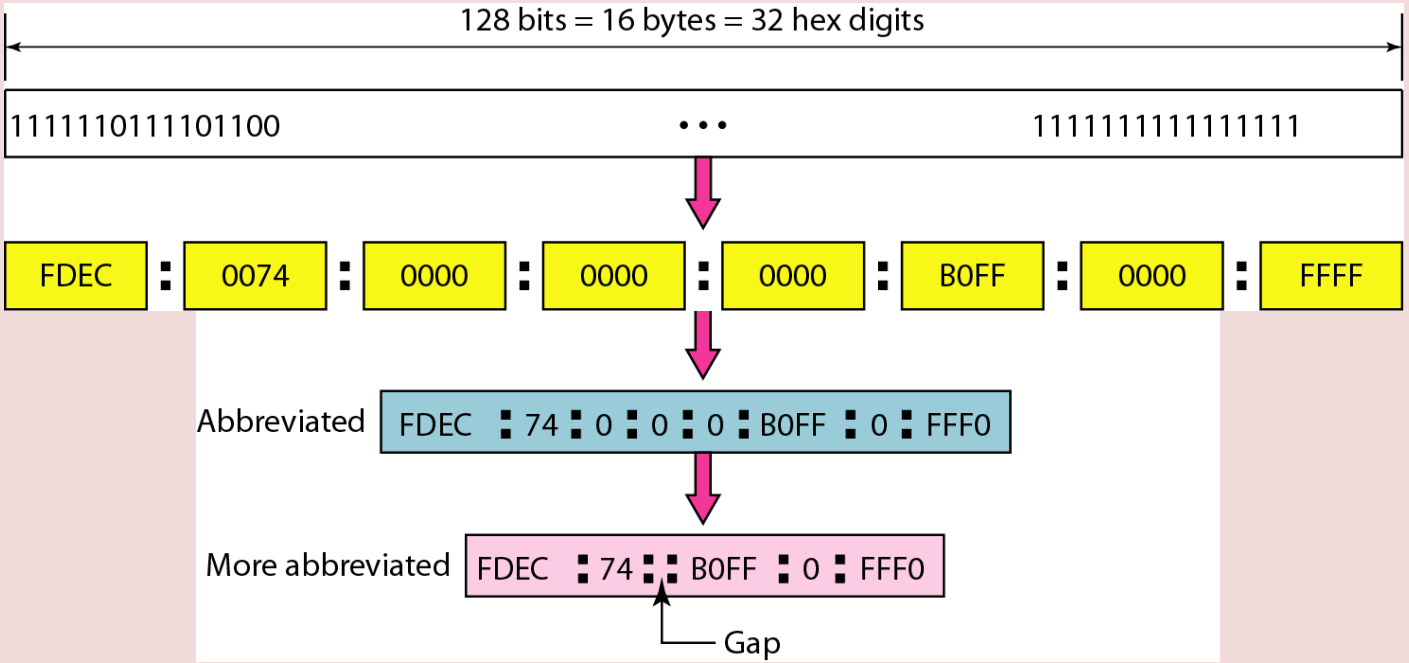
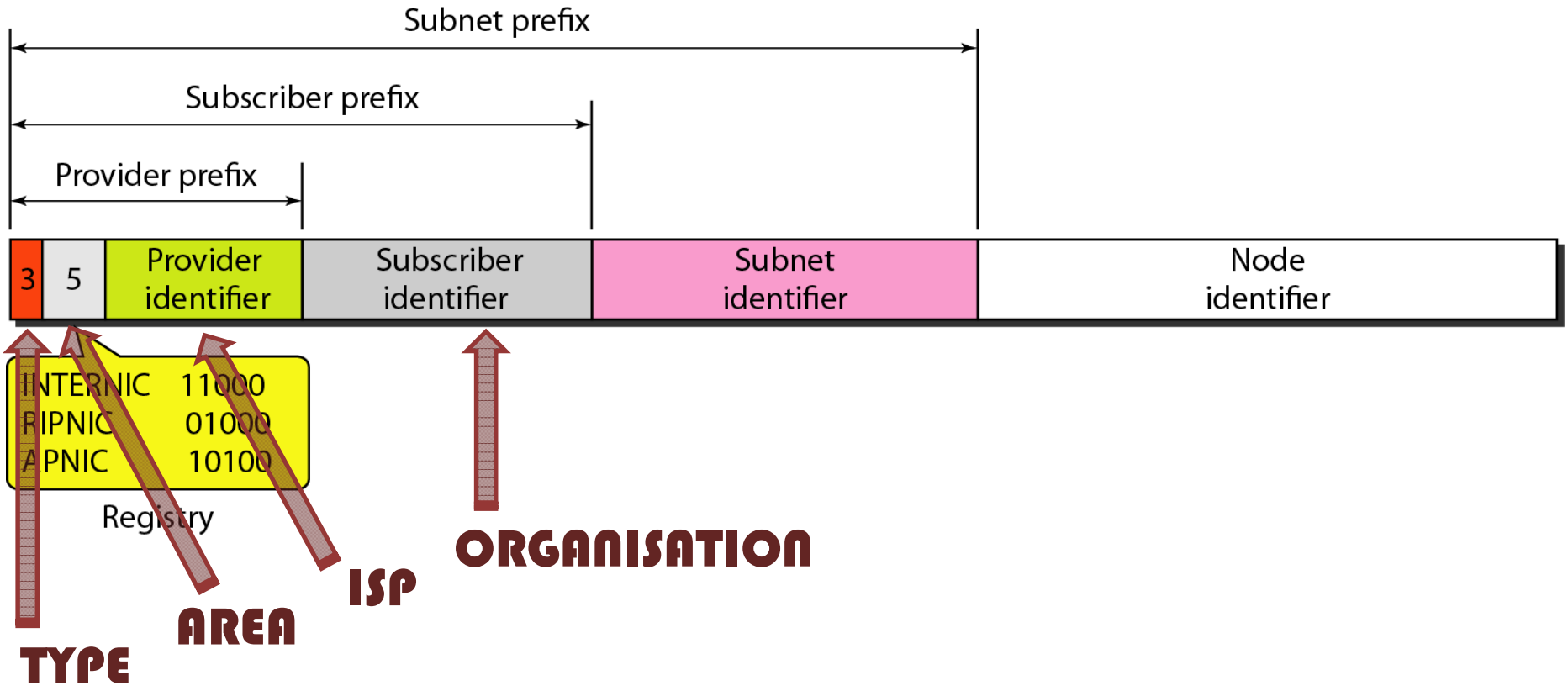


Table 14.3
IPv6 Address Space Usage
(use as reference)

Address Type	Binary Prefix	IPv6 Notation	Fraction of address space
Embedded IPv4 address	00…1111 1111 1111 1111 (96 bits)	::FFFF/96	2^{-96}
Loopback	00…1 (128 bits)	::1/128	2^{-128}
Link-local unicast	1111 1110 10	FE80::/10	1/1024
Multicast	1111 1111	FF00::/8	2/256
Global unicast	Everything else		

Global unicast addresses

- Note the hierarchy!
- Identify individual computers



On Fragmentation and Re-assembly

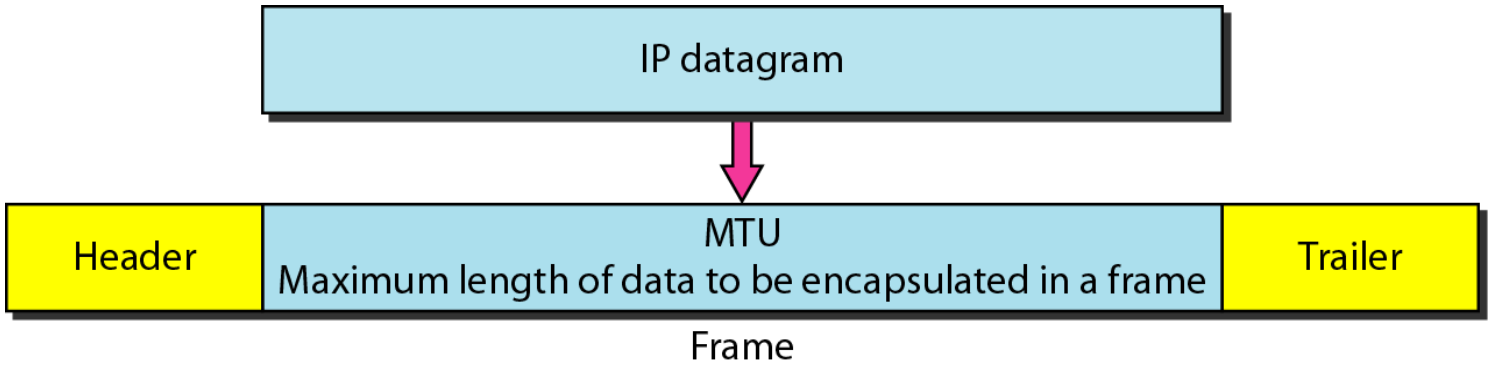
- Protocol exchanges data between two entities
- Lower-level protocols may need to break data up into smaller blocks, called fragmentation
- Reasons for fragmentation:
  - Network only accepts blocks of a certain size
  - More efficient error control and smaller retransmission units
    - Valid argument 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

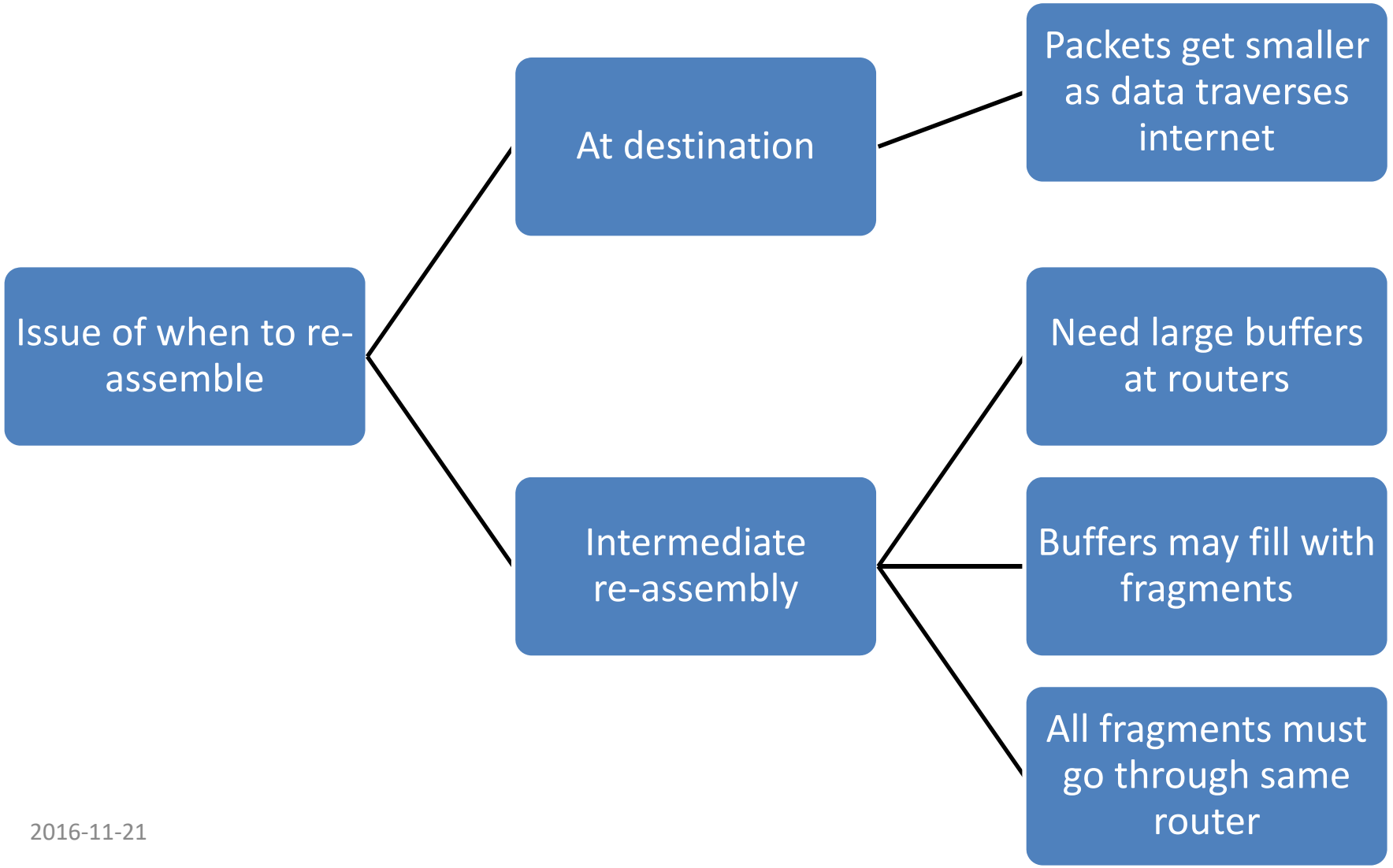
D: Do not fragment
M: More fragments

Maximum datagram size

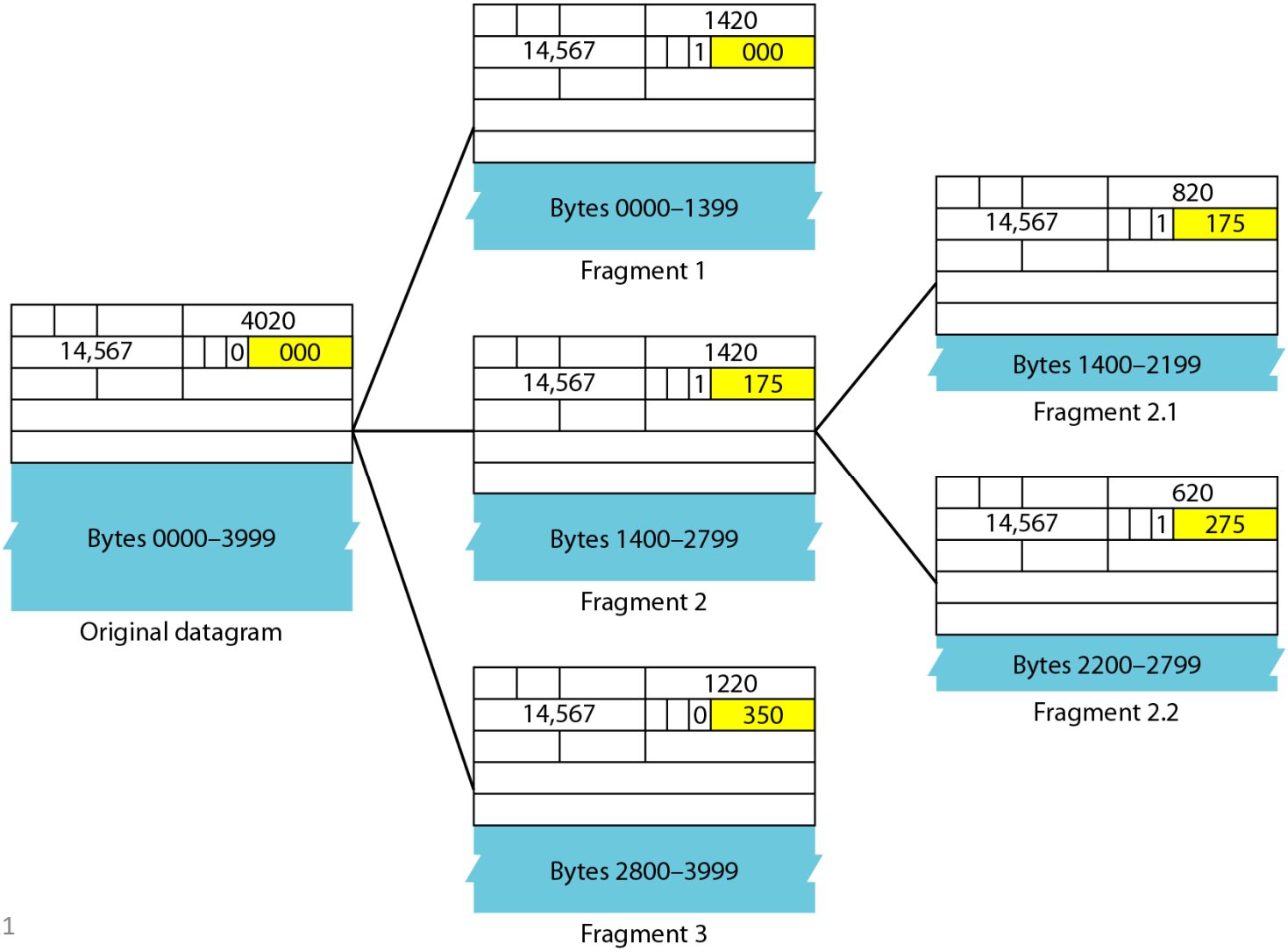


Protocol	MTU
Ethernet (802.3)	1500
Ethernet Jumbo Frames	1501 -- 9198
WLAN (802.11)	7981
PPPoE (Ethernet 802.3)	1492

Fragmentation Re-assembly

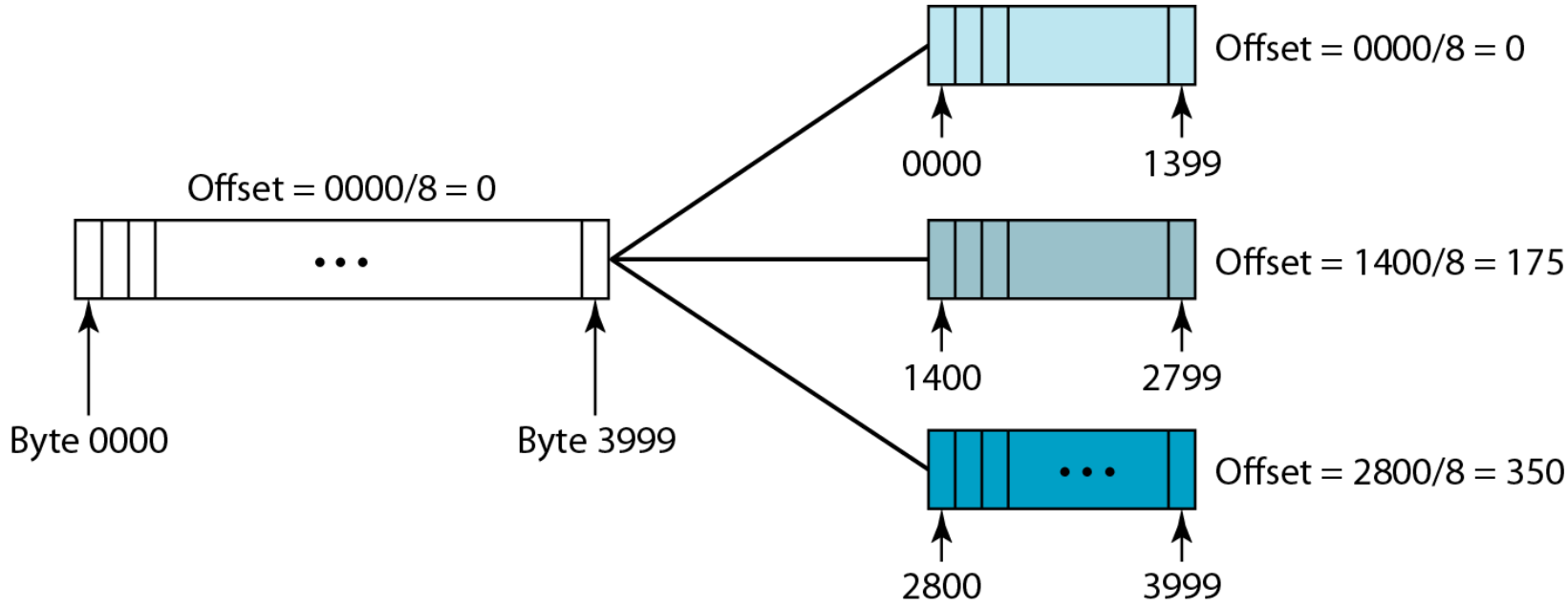


Fragmentation example



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.

What with TCP/UDP header?

- Where is a TCP or UDP header in fragments?
- Problem for Network Address and Port Translation nodes

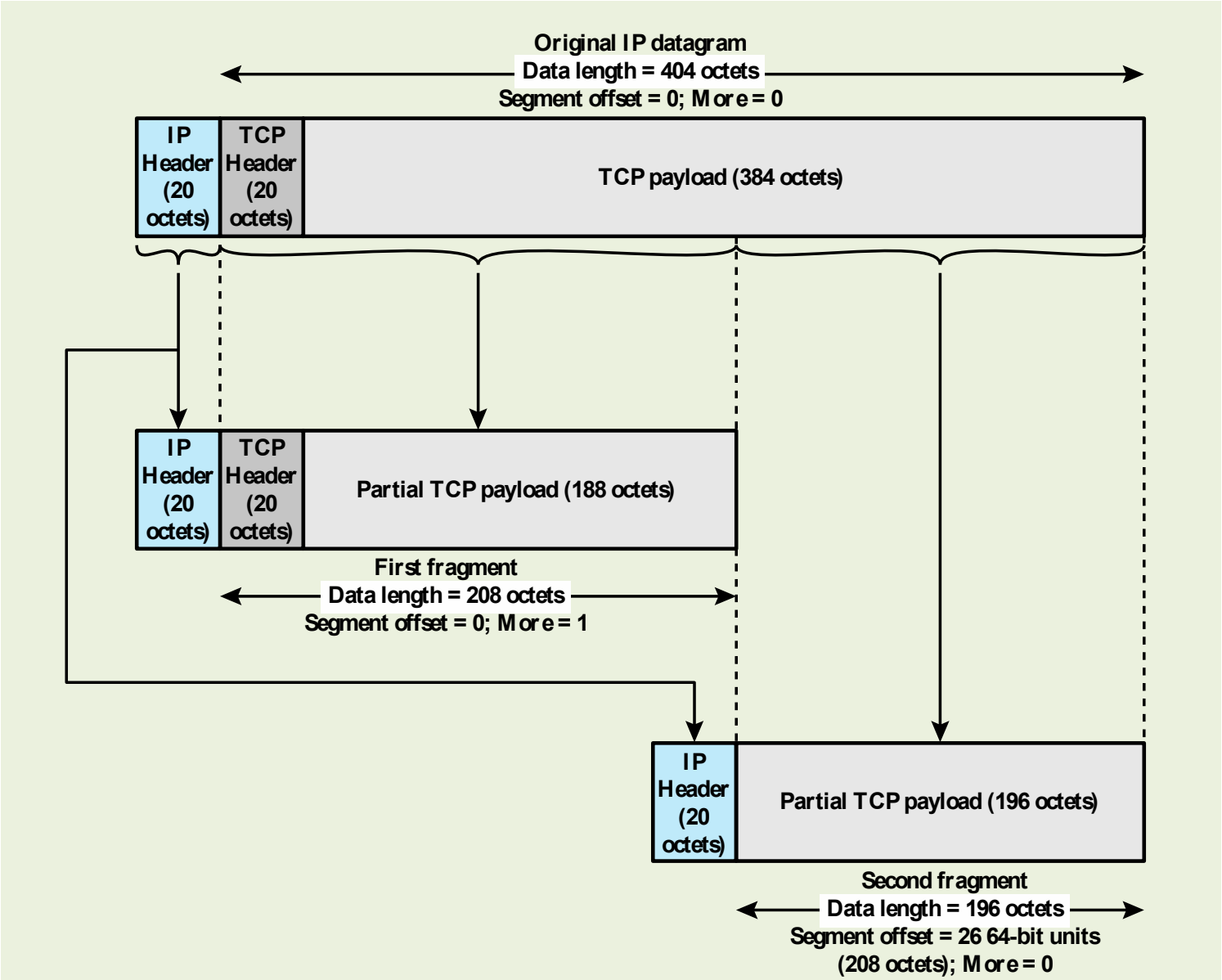
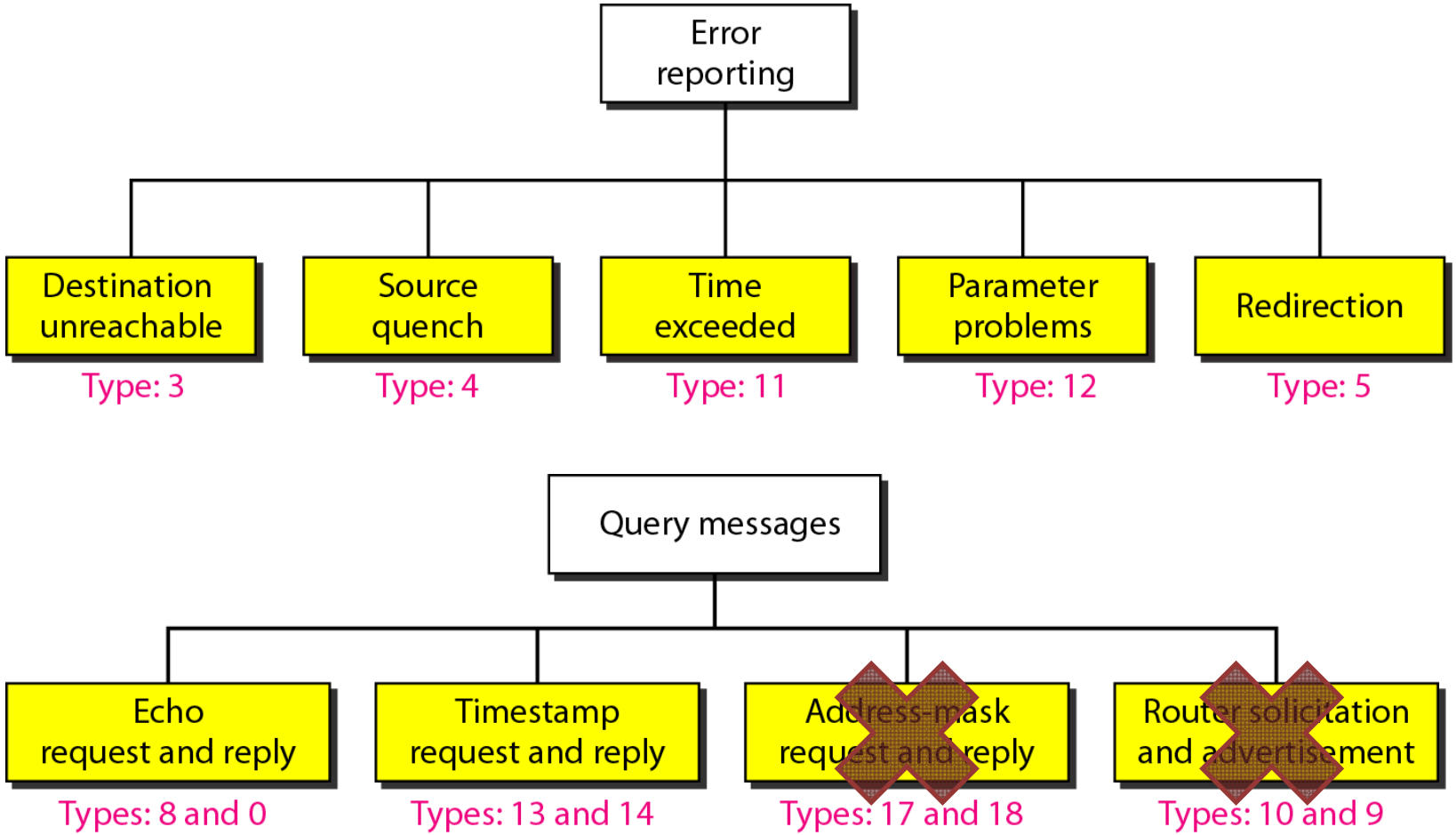


Figure 14.4 Fragmentation Example

Internet Control Message Protocol (ICMP)

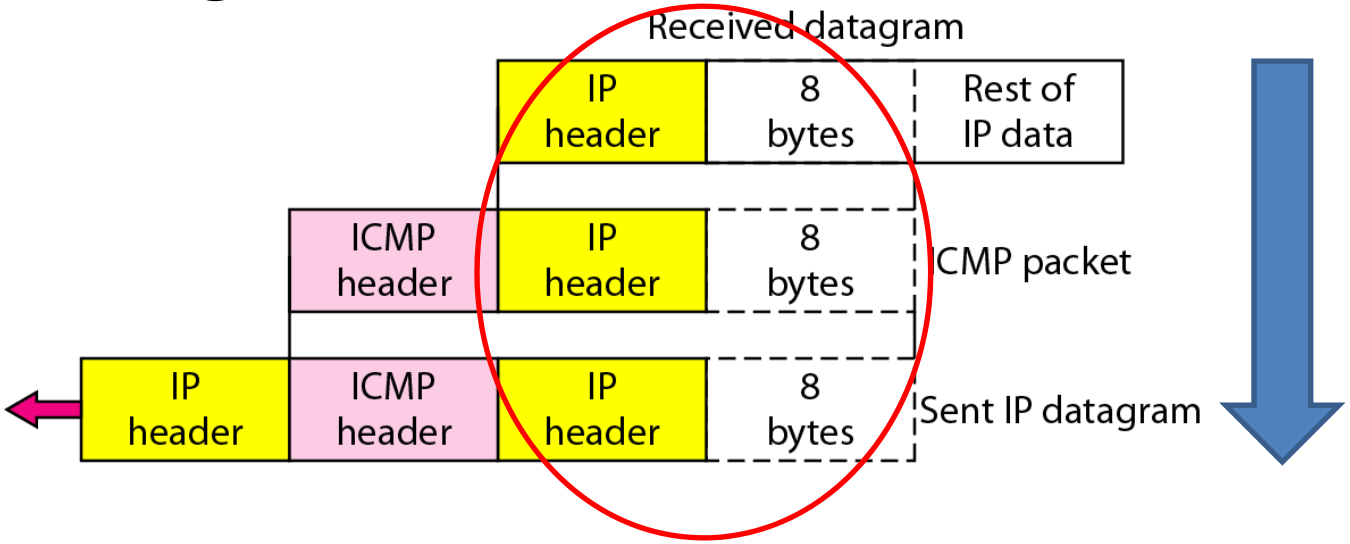
- RFC 792
- Provides a means for transferring messages from routers and other hosts to a host
- Provides feedback about problems
    - Datagram cannot reach its destination
    - Router does not have buffer capacity to forward
    - Router can send traffic on a shorter route
- Encapsulated in IP datagram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

ICMPv4 message types

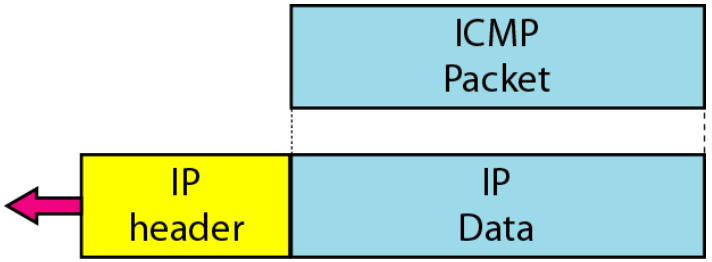


ICMP message formats

- Error reporting



- Query messages



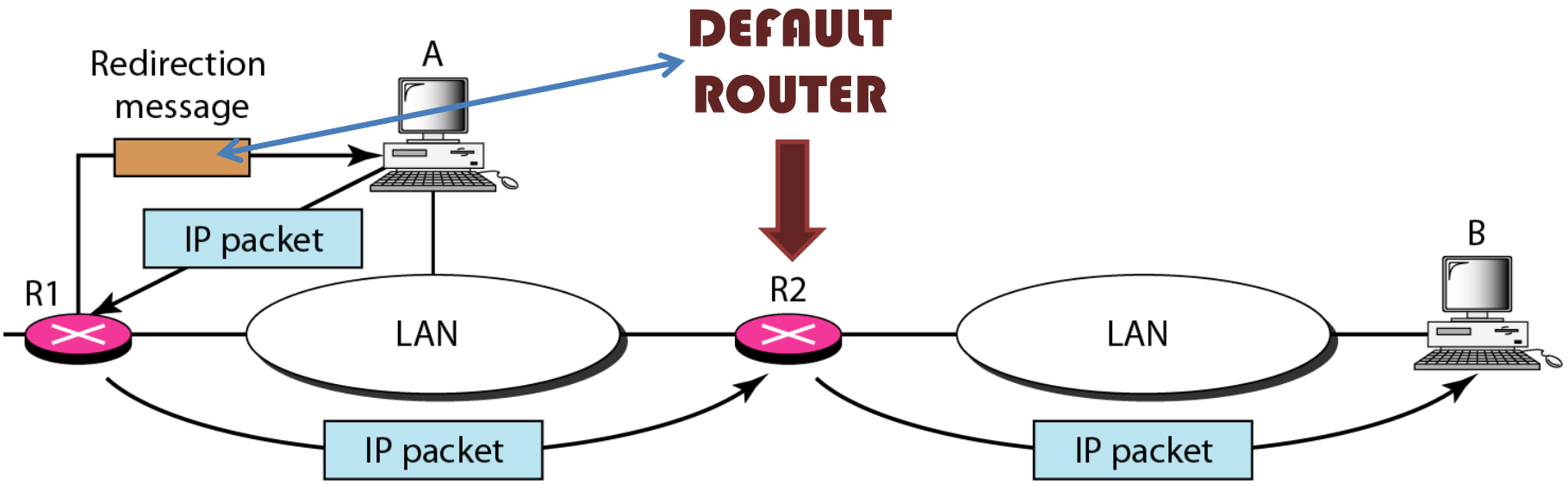
Echo request and reply (query type)

- Is my destination alive?

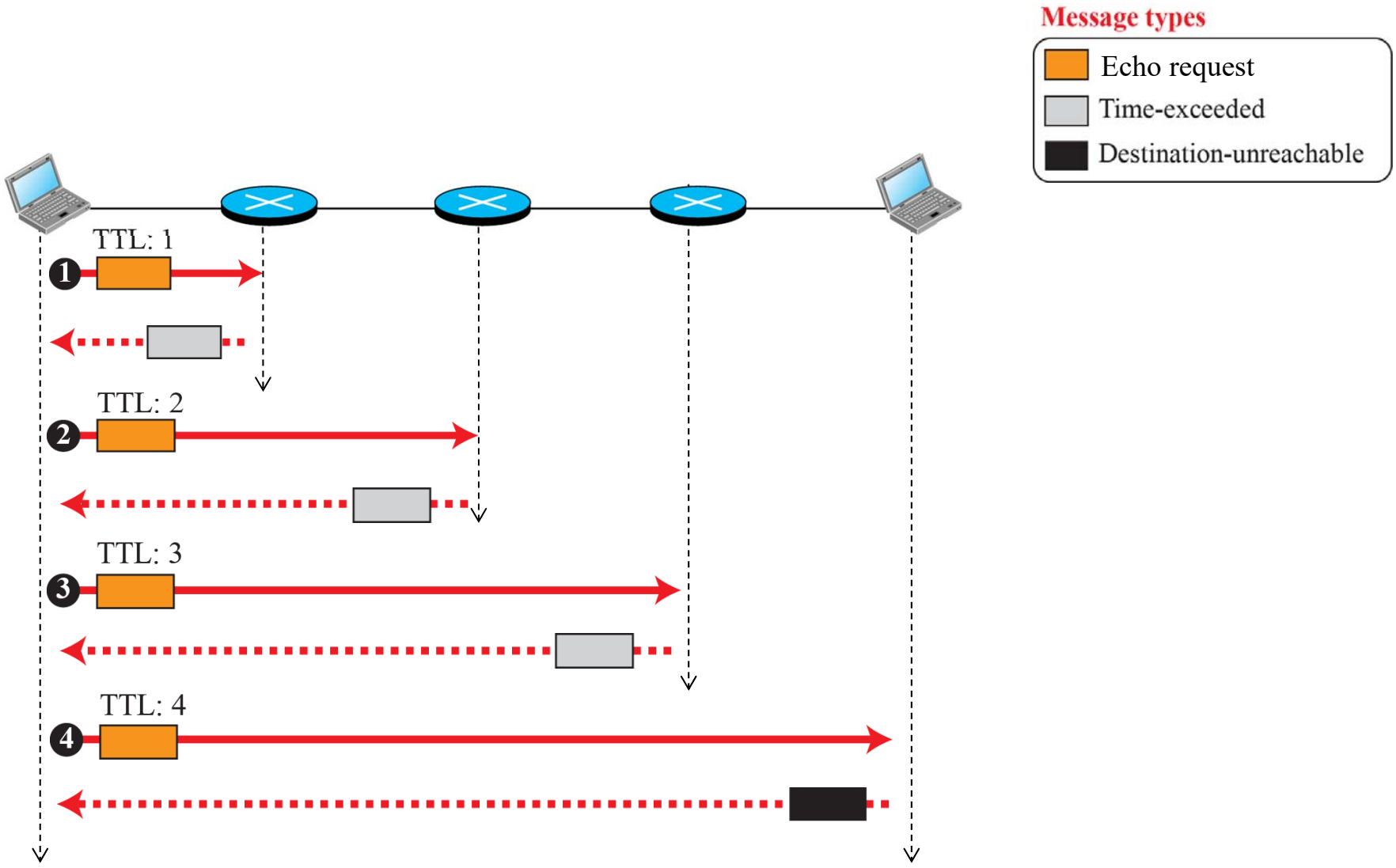
- Network diagnostics
  - IP layer
- Debugging tools
  - Ping
  - Traceroute

Redirection (error reporting type)

- Routing update for hosts
  - Security/reliability?



Traceroute


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

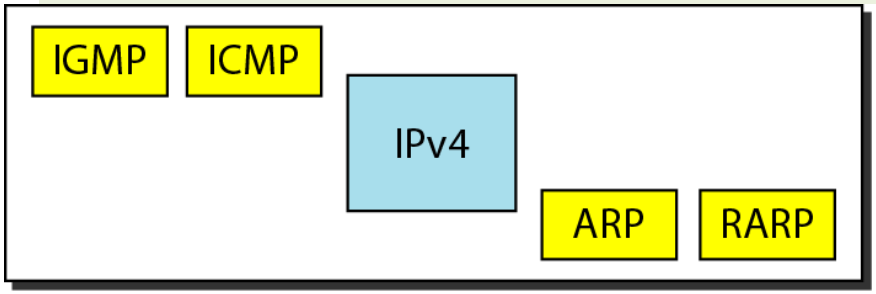
ICMPv6

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

Changes to ICMP

ICMPv4

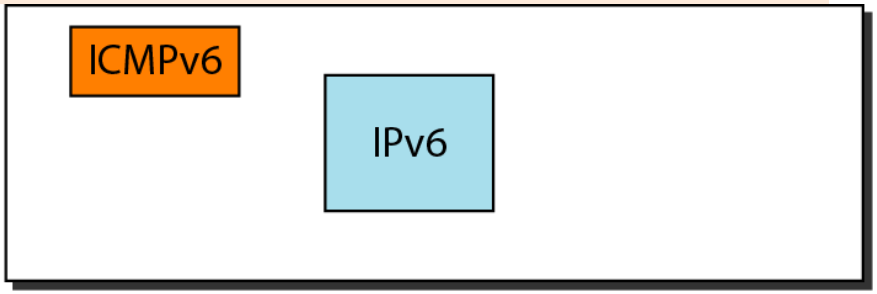
- Some unused functions



Network layer in version 4

ICMPv6

- Same principle
- Some new functions
- Convergence
- Suits IPv6 better



Network layer in version 6

Neighbour Discovery Protocol (NDP)

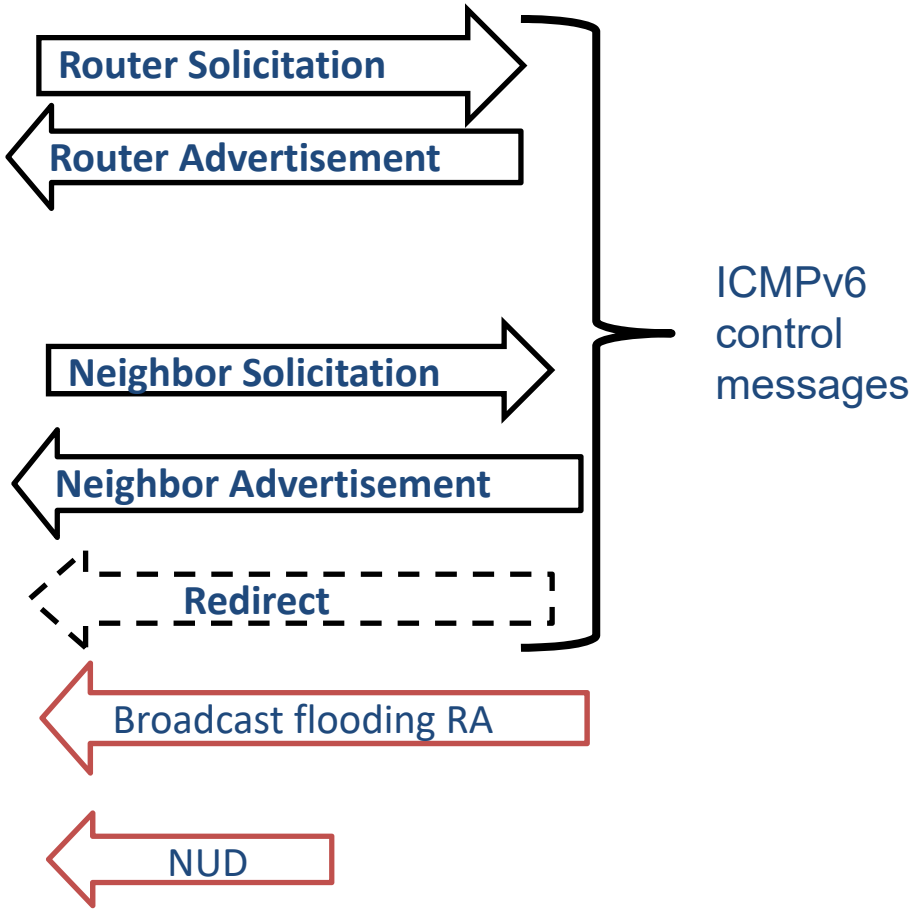
- Router Solicitation/Adverticement
  - Find a router = ”default gateway”
  - Announce router = ”default gateway”
- Neighbour Solicitation/Adverticement
  - Same functionality as IPv4 ARP
  - Also Address Auto Configuration
    - Suggest own address
    - Check for duplicates

IPv6 StateLess Address Auto Configuration (SLAAC)

- Every NIC has several IPv6 addresses
  - Most have Link Local Address
- Creation of Link Local Address:
  - Use MAC address
  - Prebend with wellknown prefix fe80::/64
  - Check for duplicates

ICMPv6 ND and AAC

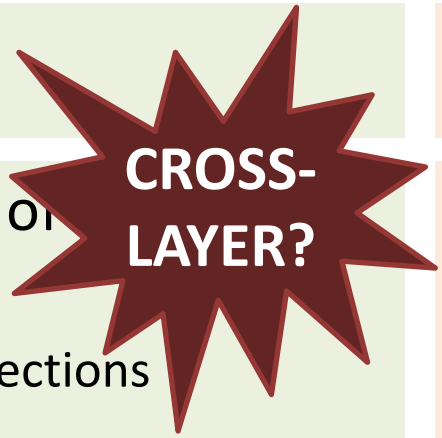
1. Router Discovery
2. Address Configuration Mechanism (RFC 4862)
3. Address Resolution
4. Duplicate Address Detection
5. Updating a change of MAC address to the network
6. Neighbor Unreachability



IPv6 and QoS

Flow label

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

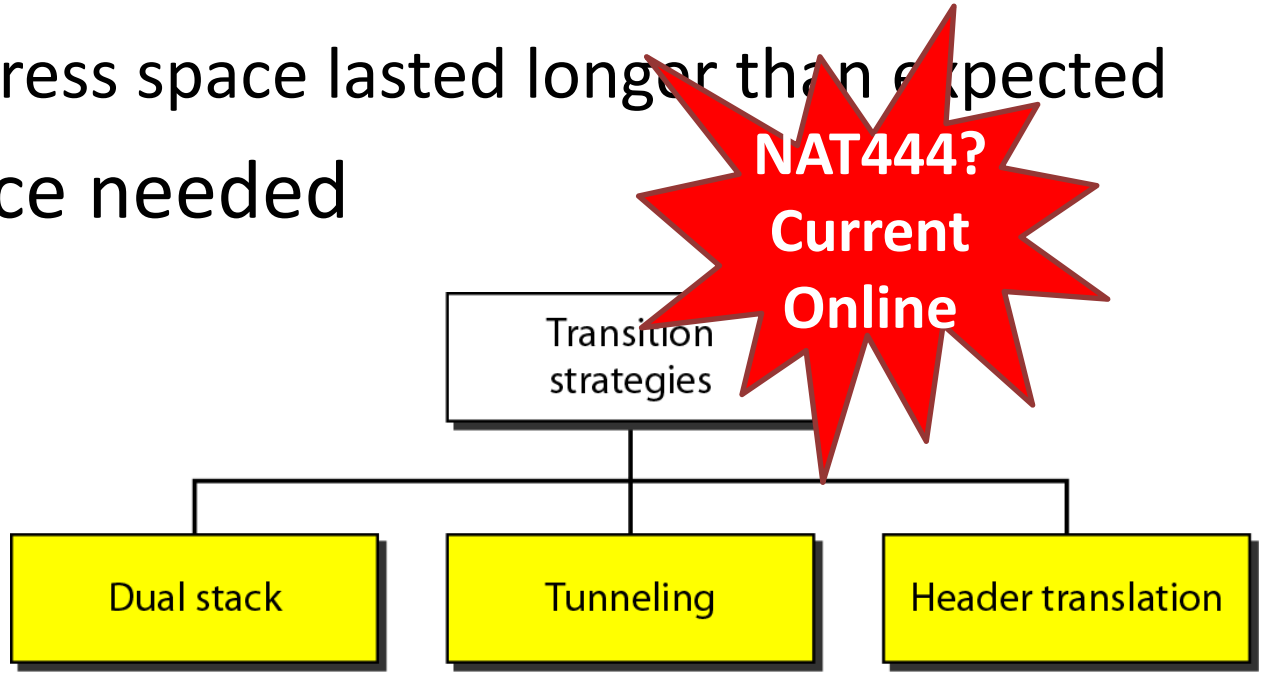


Traffic class

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

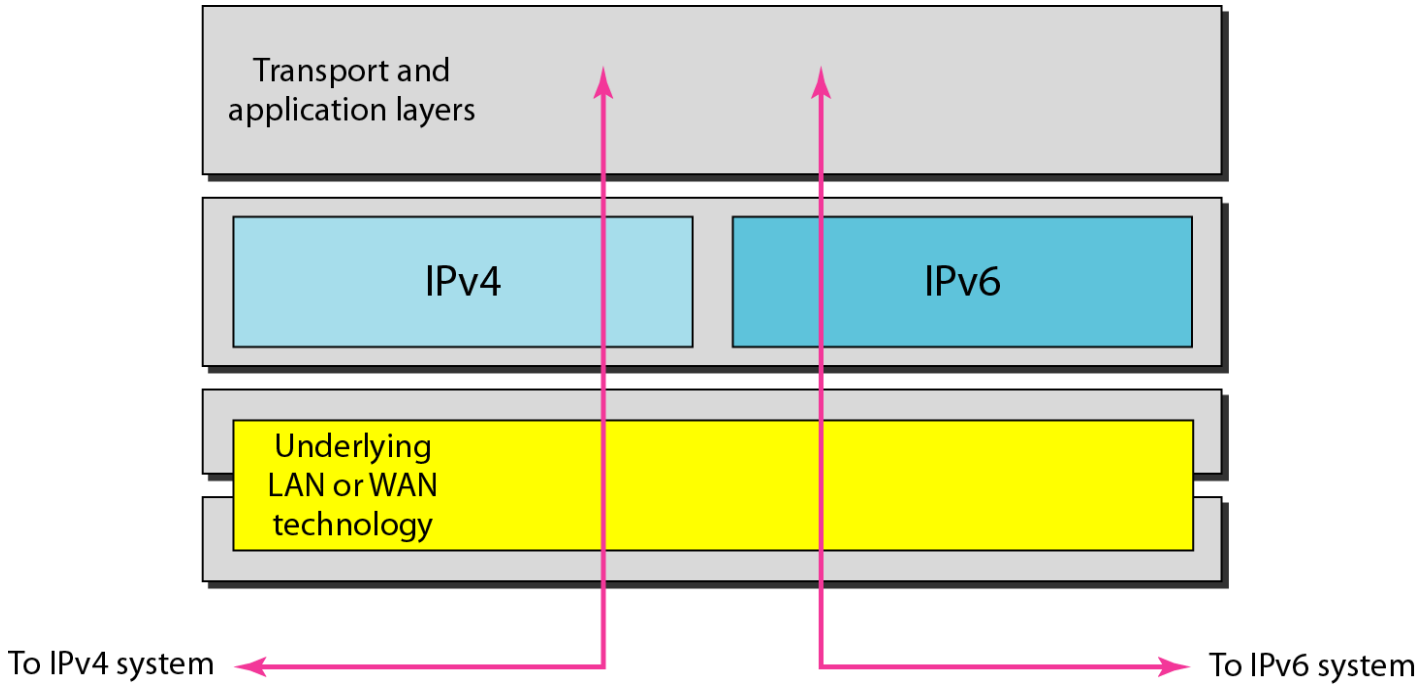
Transition: IPv4 → IPv6

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



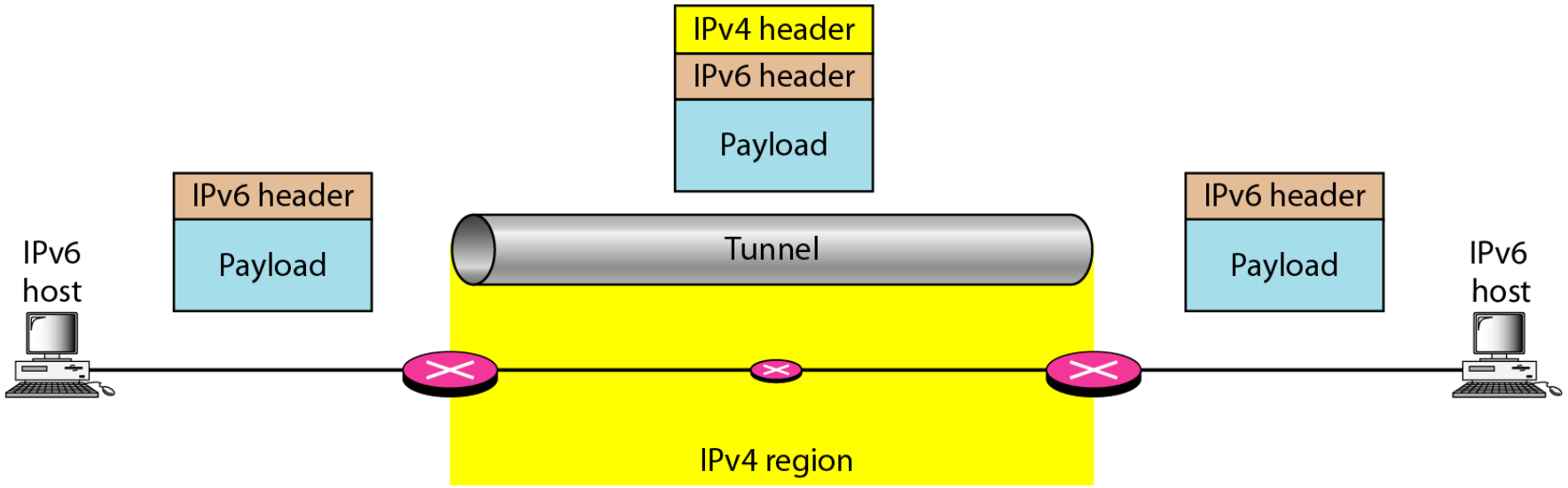
Transition: (1) Dual stack

- Decision based on destination IP



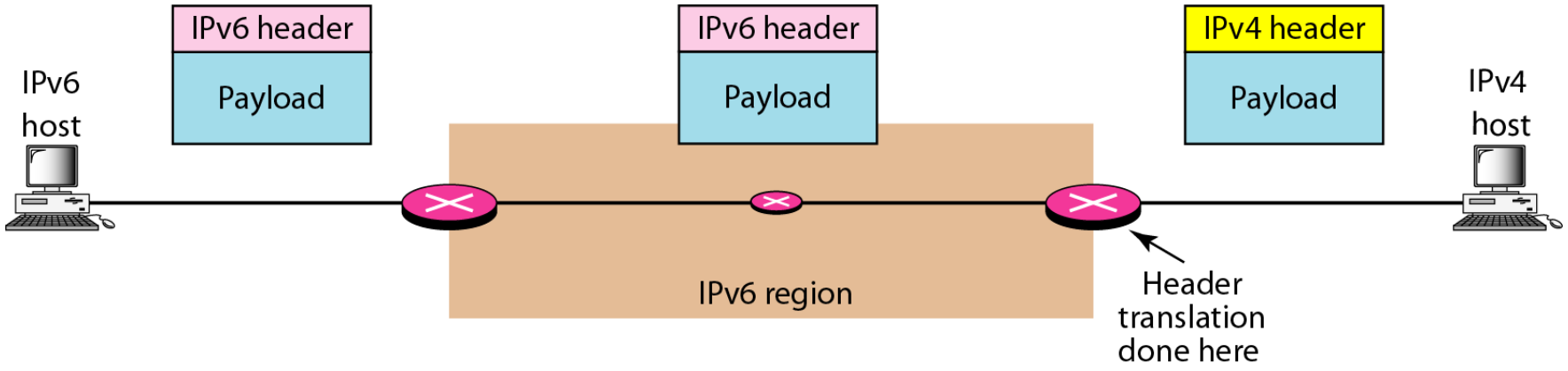
Transition: (2) Tunneling

- A few IPv6 routers



Transition: (3) Header translation

- A few IPv4 routers



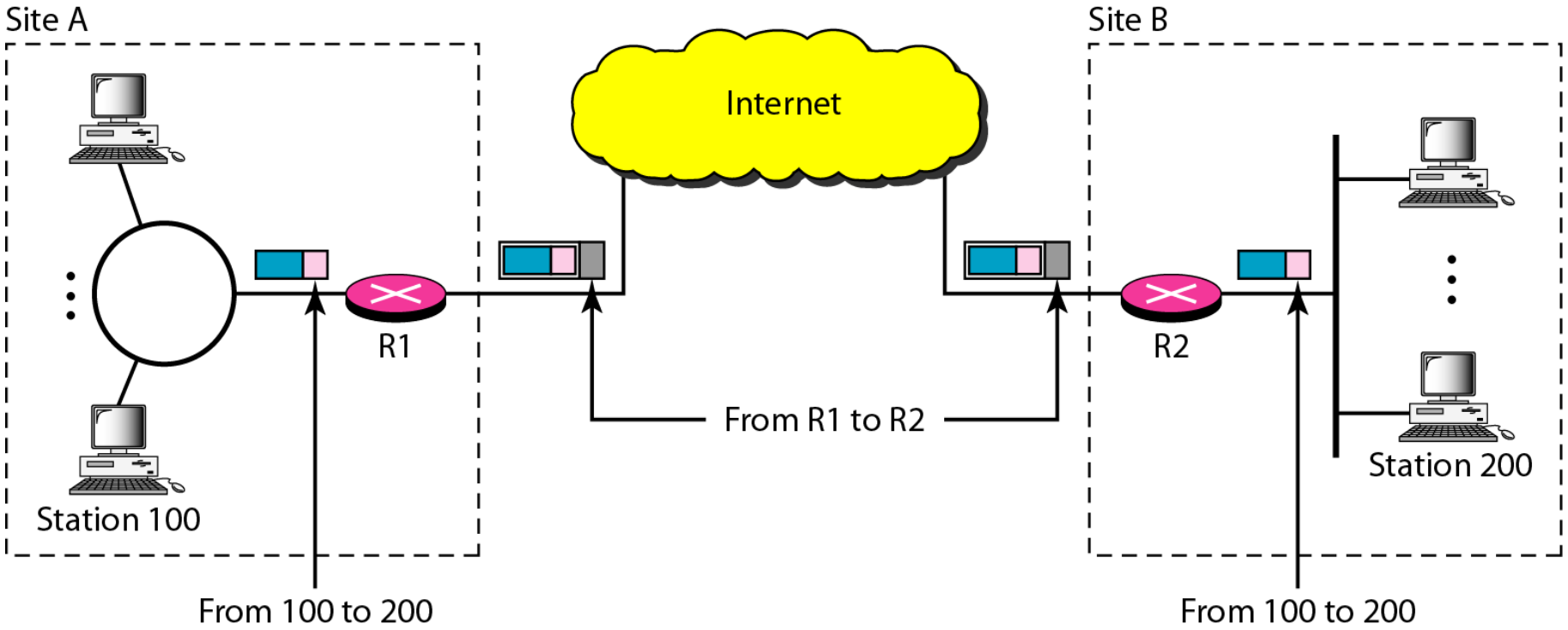
Virtual Private Network (VPN)

- 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

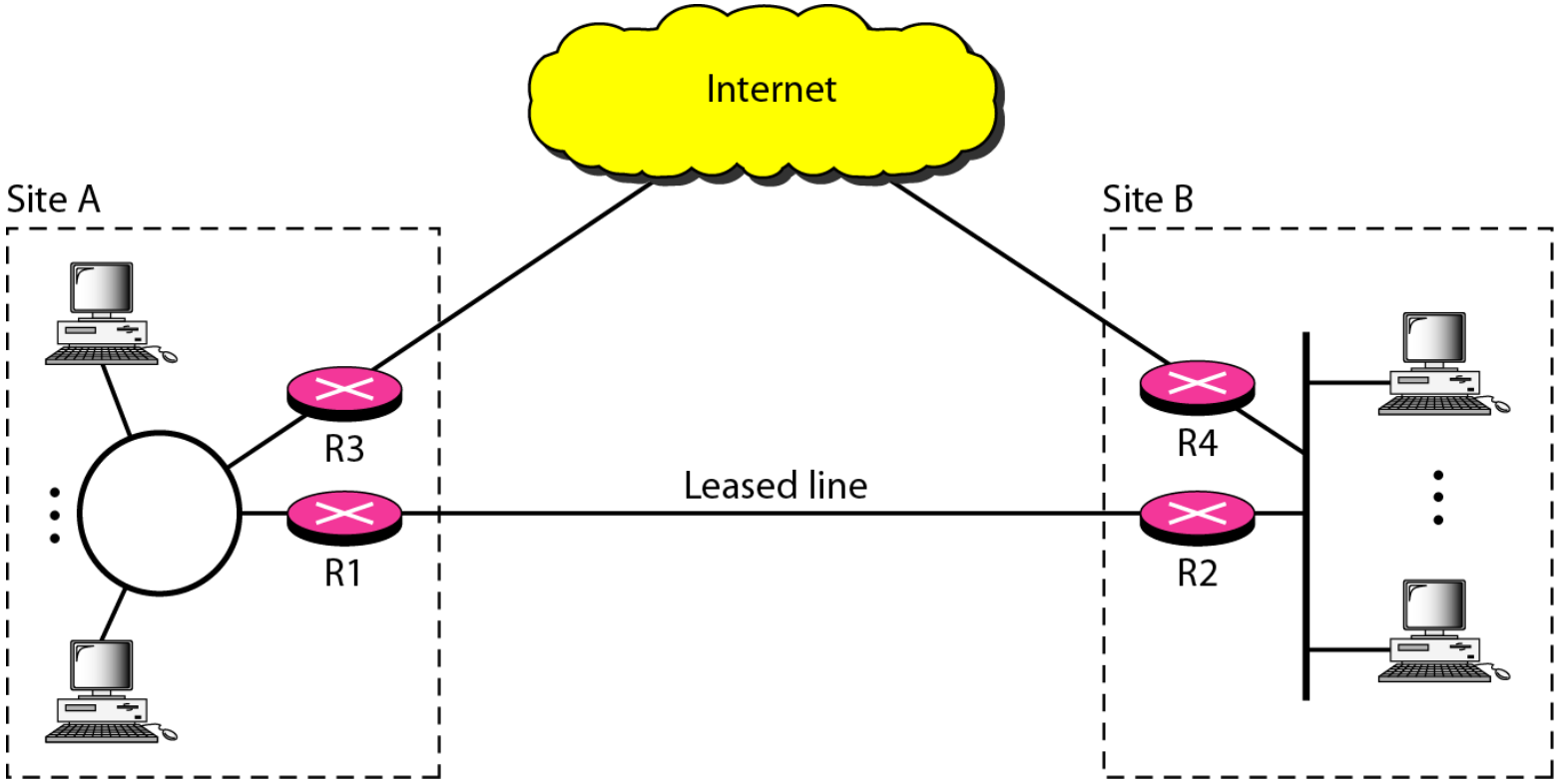
An example VPN

- IPSec between routers



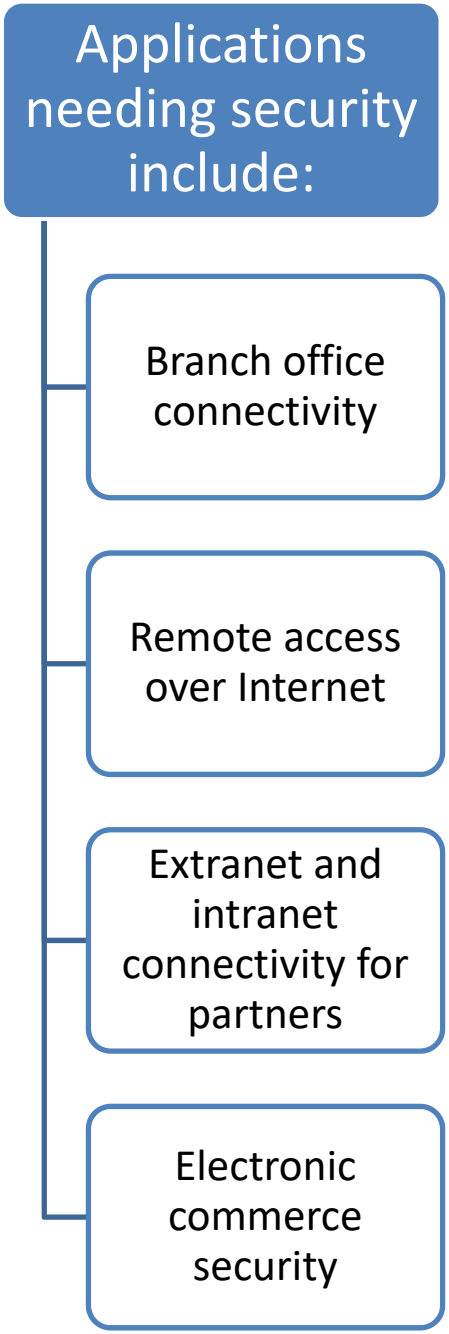
Virtual Private Network (VPN)

- Overlay network
- Alternative to a real private network



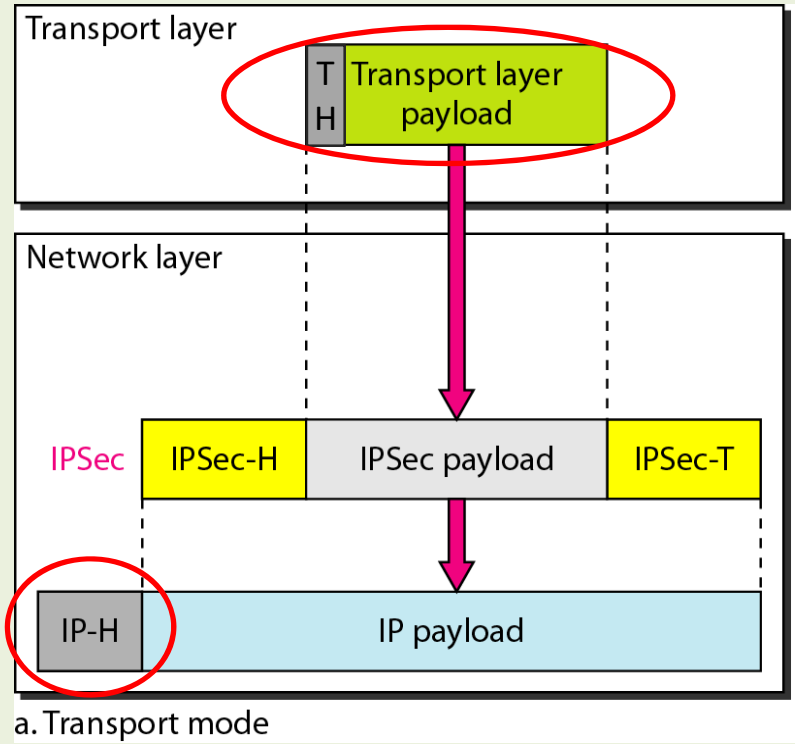
IPsec

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



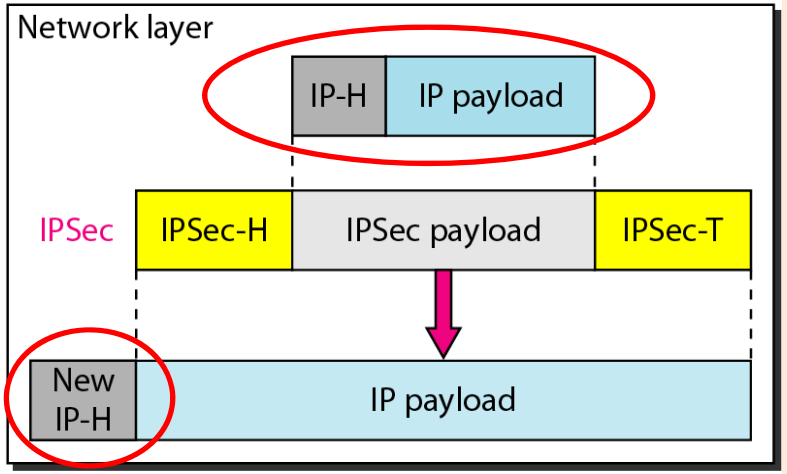
IPSec

Transport mode



a. Transport mode

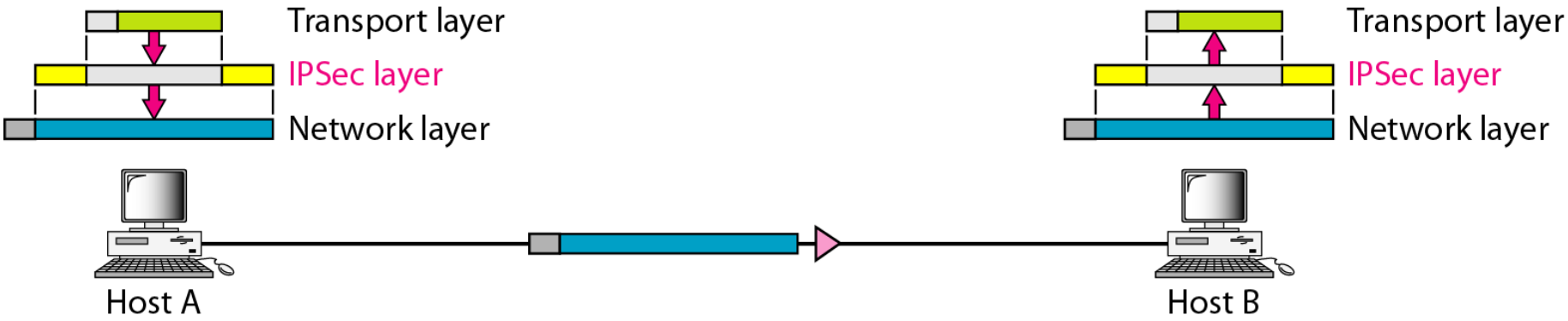
Tunnel mode



b. Tunnel mode

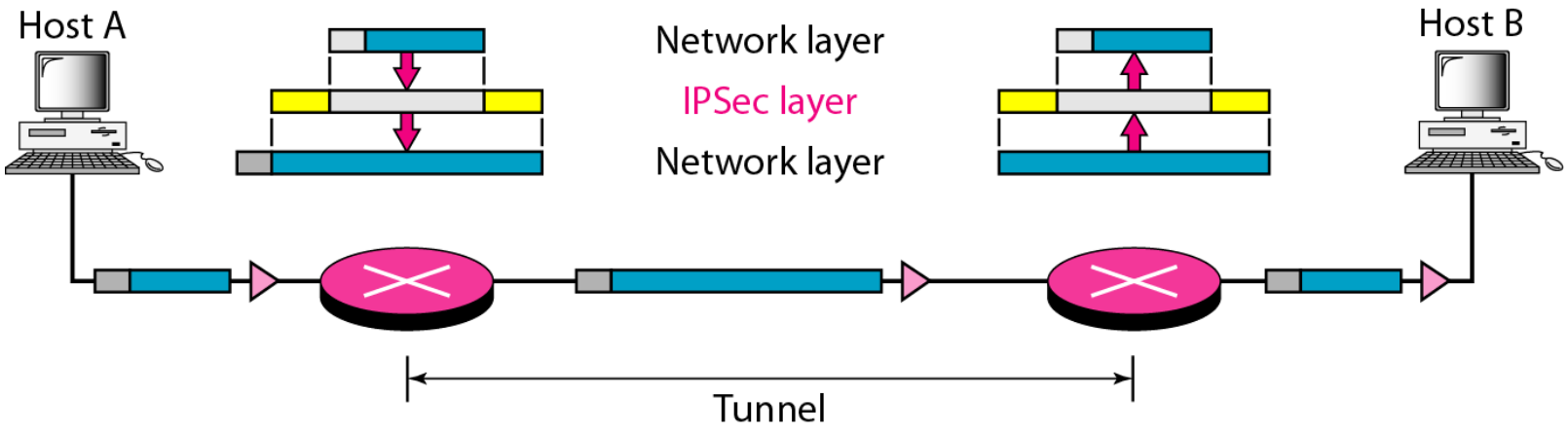
Transport mode in action

- Data protected
- Headers unprotected
  - Addresses fully visible

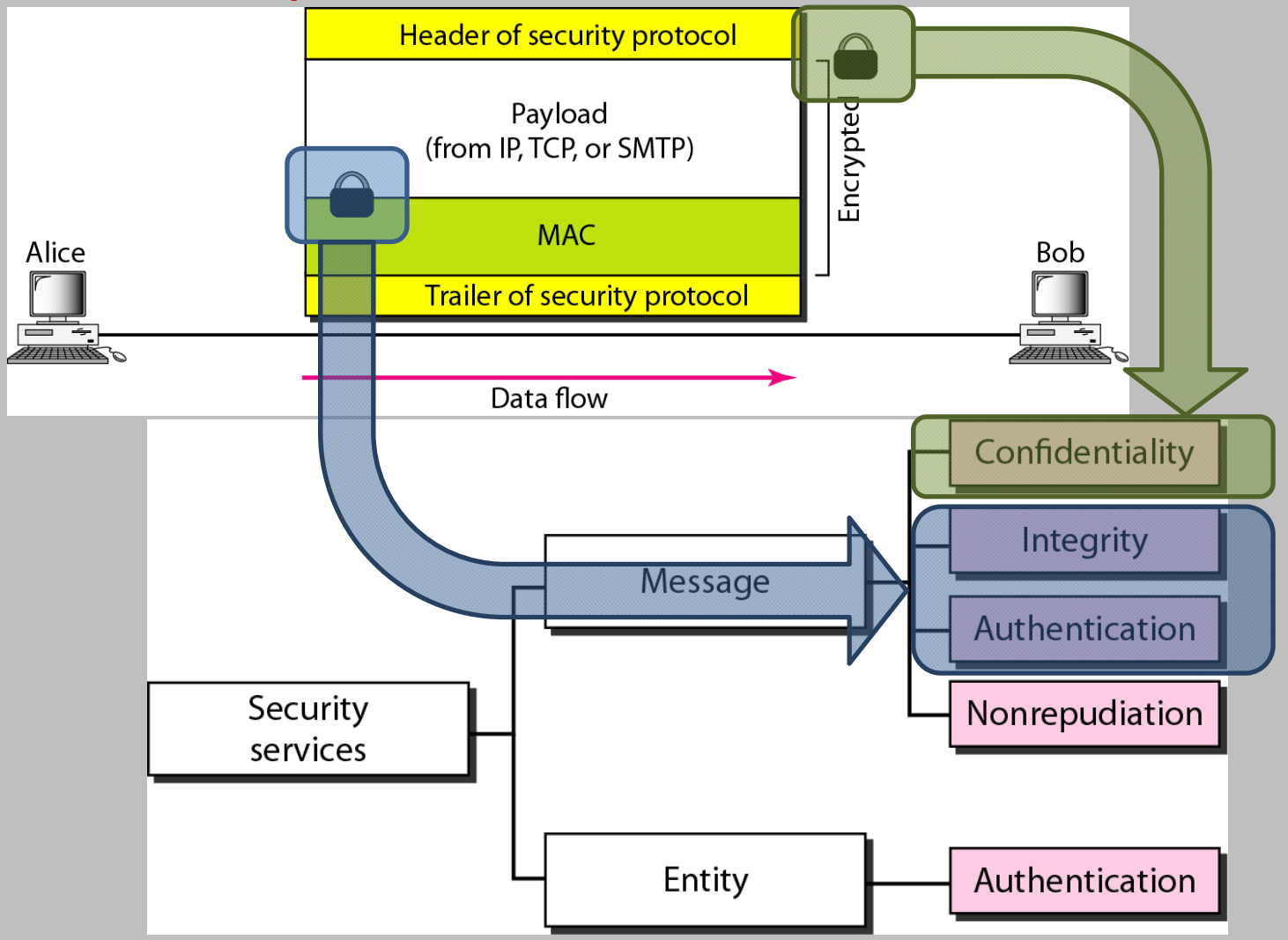


Tunnel mode in action

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



Internet security (discussed in other courses)



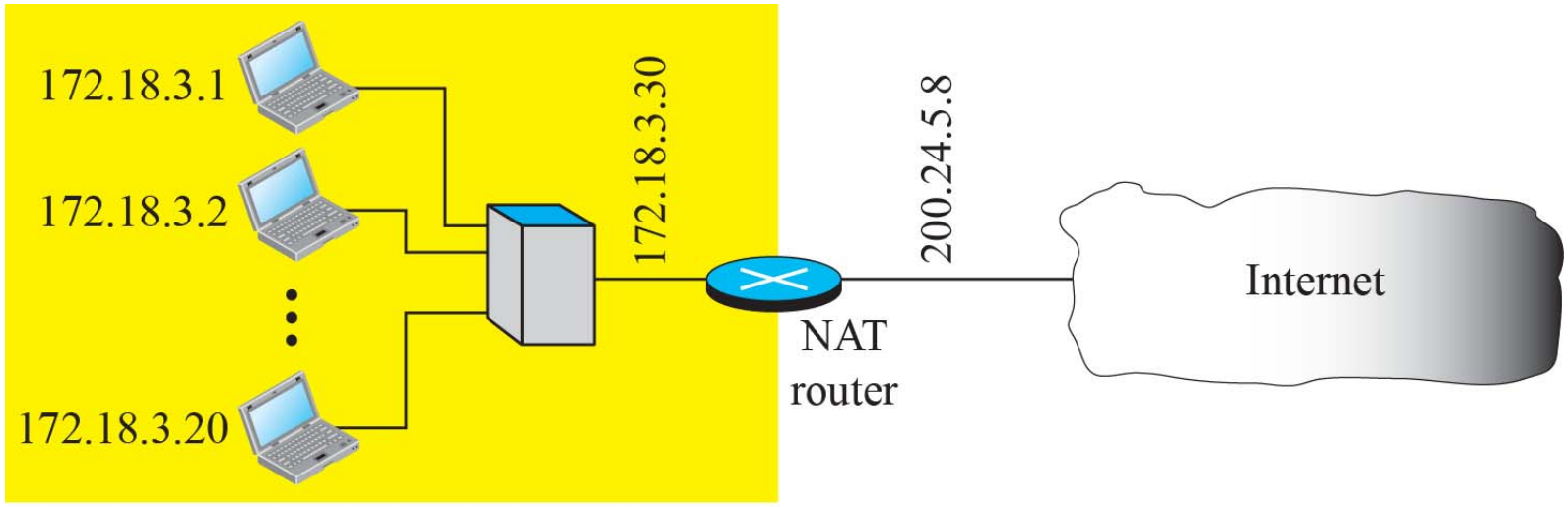
VPN alternatives (bonus material)

- 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

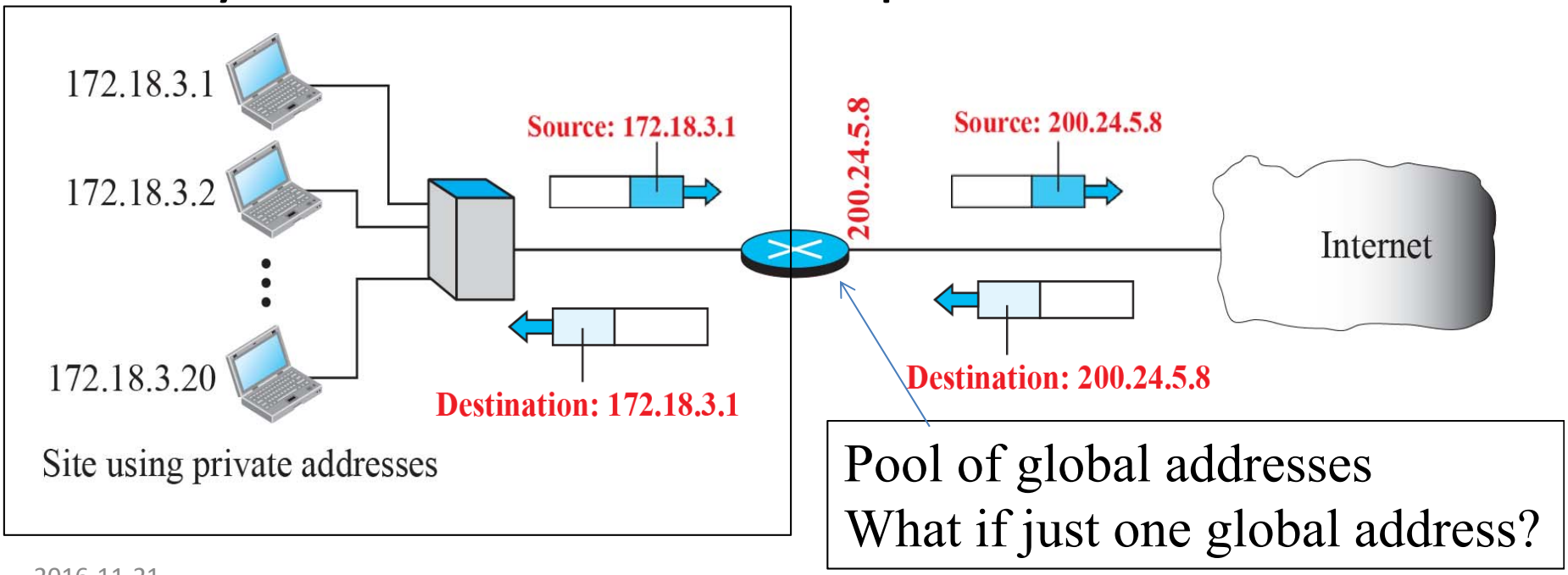
- Sharing of routable addresses (scarse resource)
- Adds some security …



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



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

NAT444, Carrier Grade NAT

- Carrier performs NAT in core
- Benefits?
- Problems?
- Online discussion 2