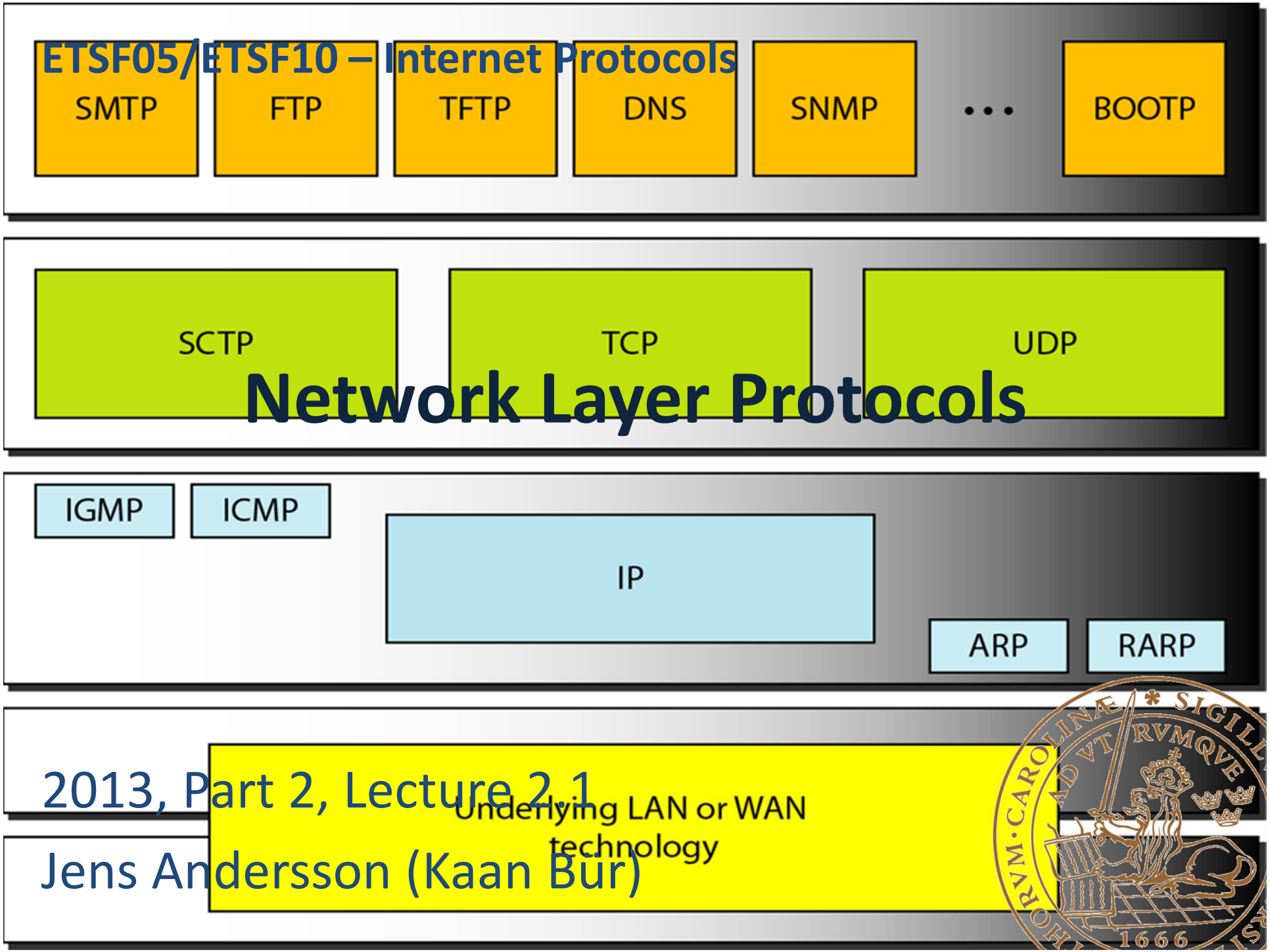
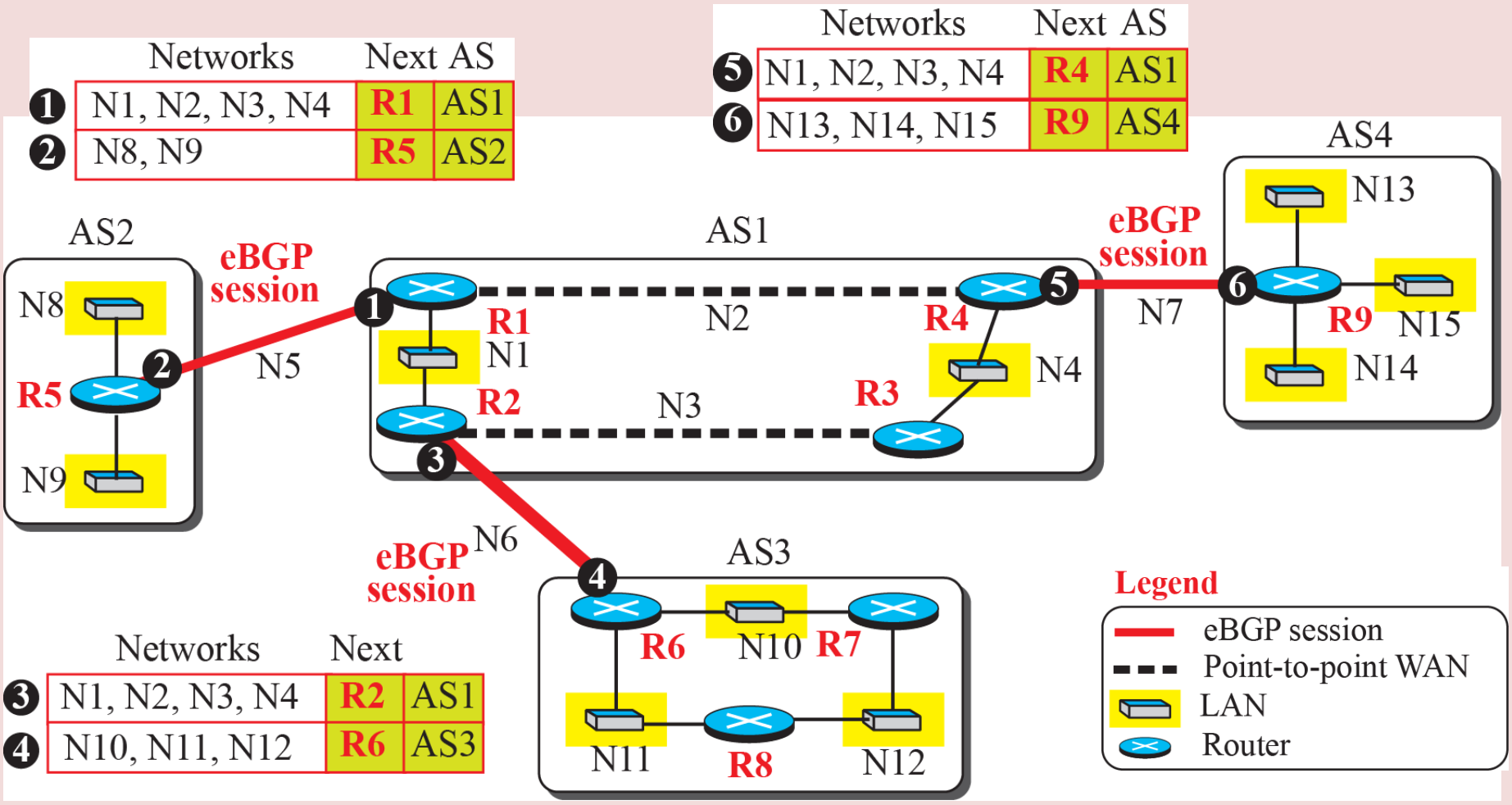
ETSF05/ETSF10 – Internet Protocols



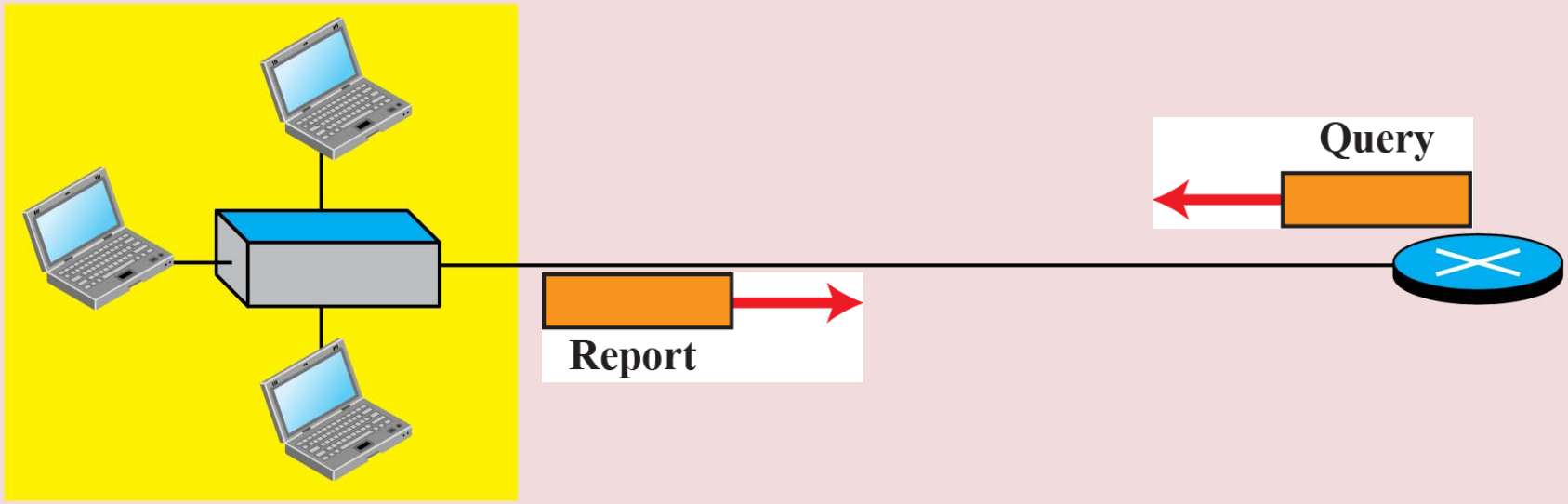
2013, Part 2, Lecture 2.1

Jens Andersson (Kaan Bür)

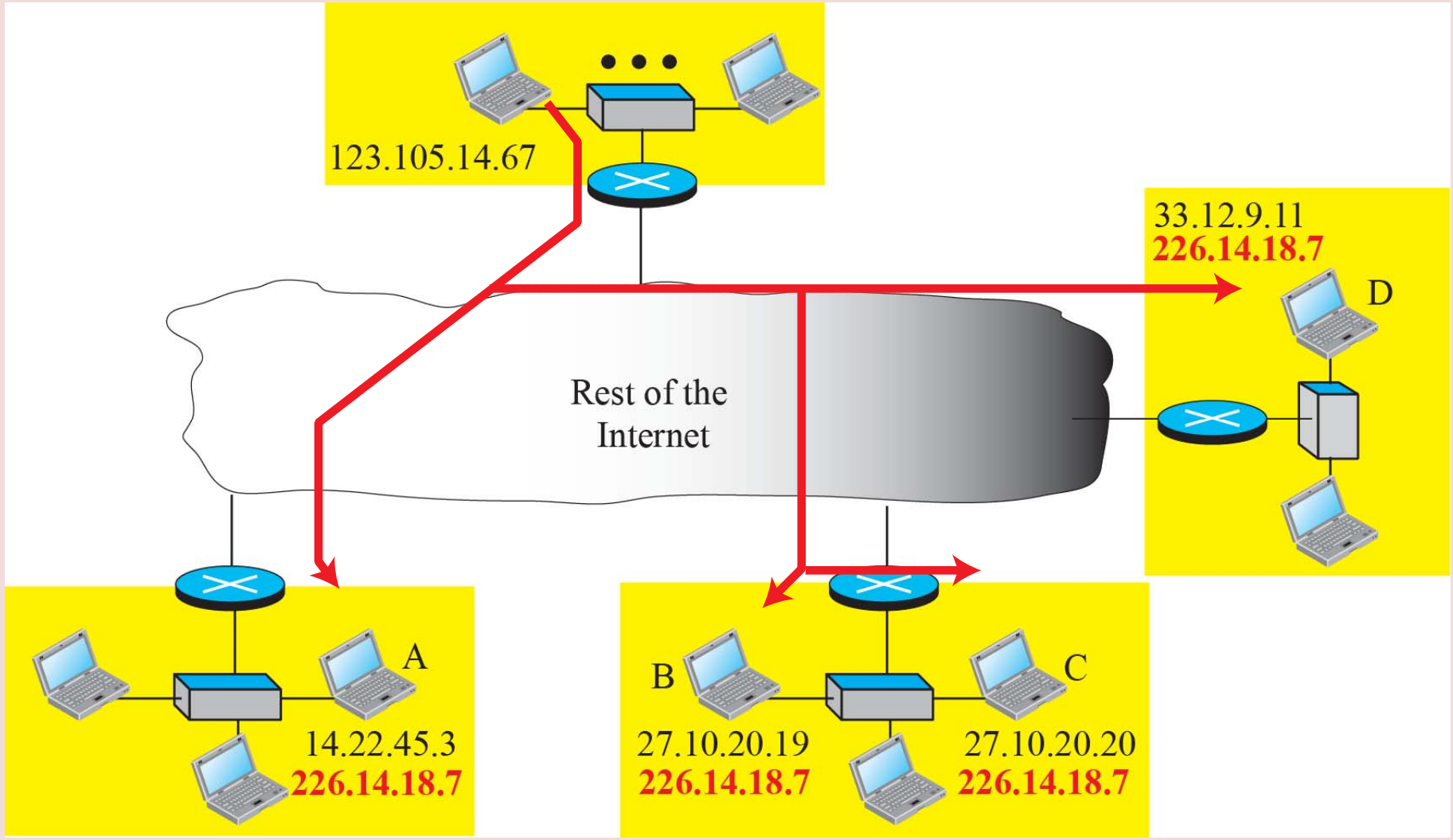
Route Transfer



Scope of IGMP

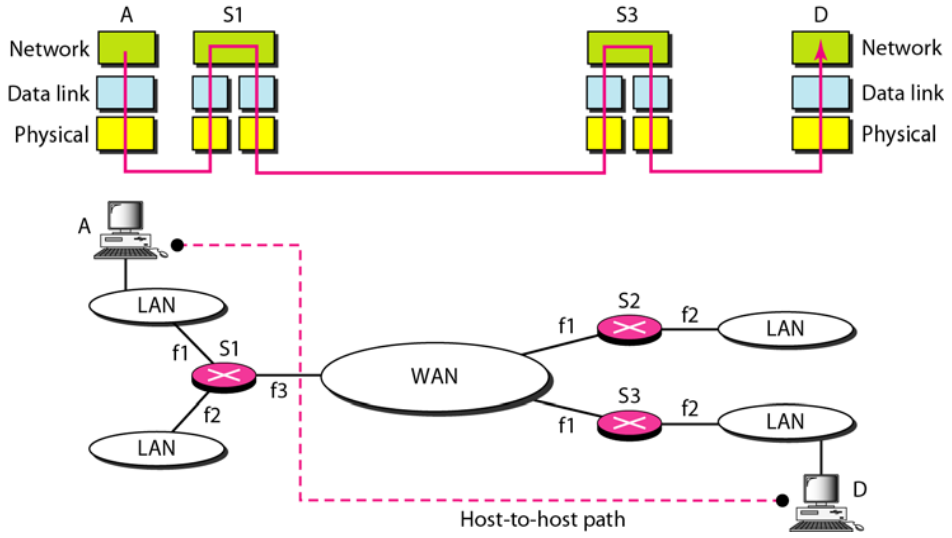


IGMP: Designated/Parent Router



Network layer

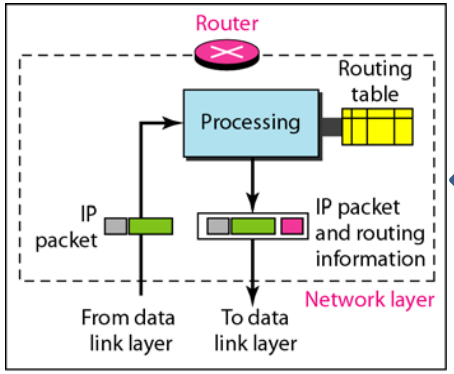
- L3 is end-to-end



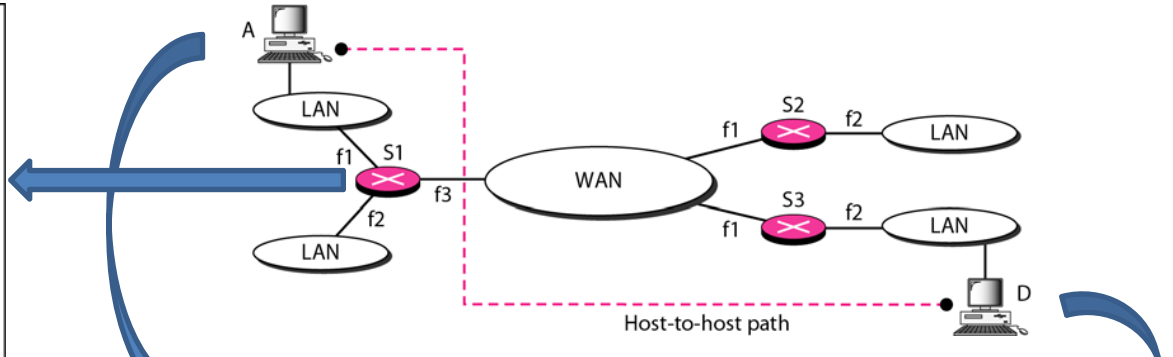
- L2 is host-to-host

Network layer: Routing

- L3 is end-to-end

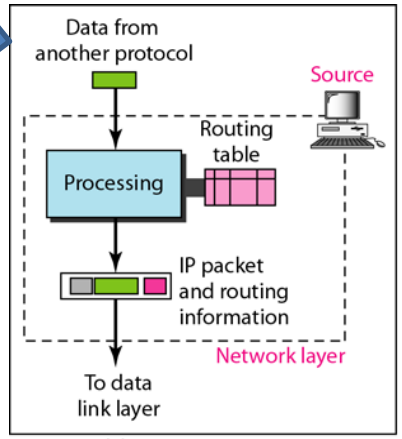


c. Network layer at a router

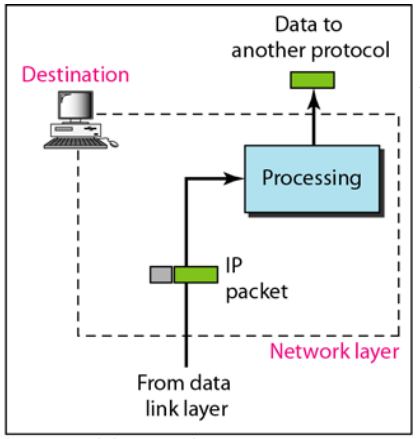


Two functions:

1. Finding best path
2. Forwarding

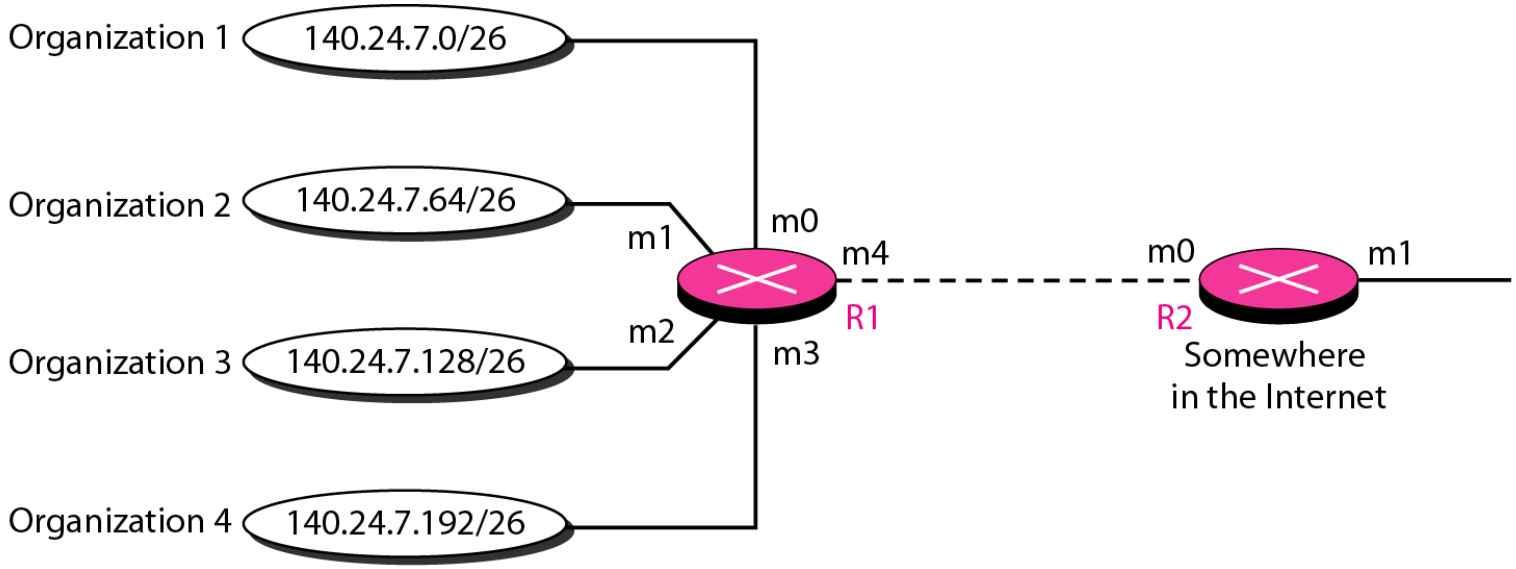


a. Network layer at source



b. Network layer at destination

Forwarding: Address aggregation



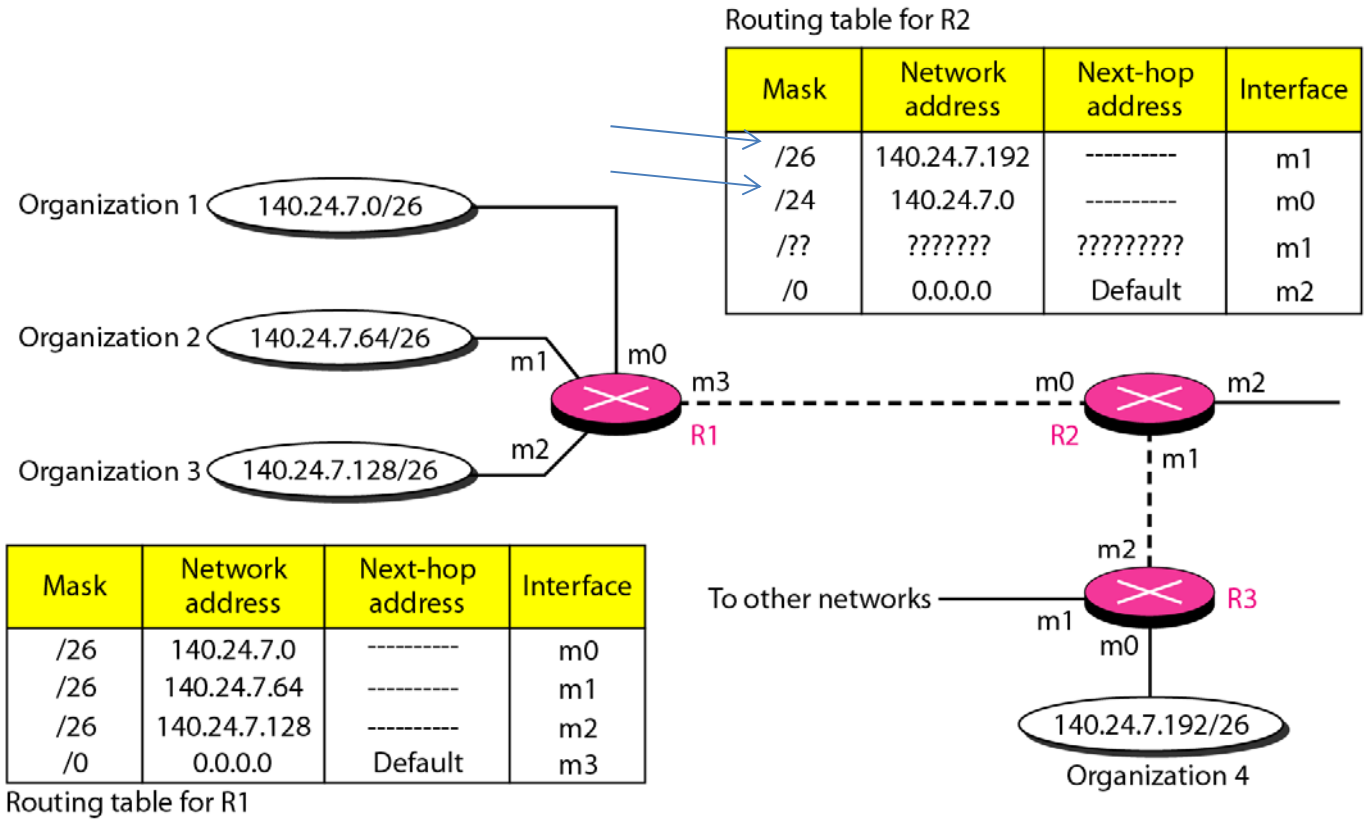
Mask	Network address	Next-hop address	Interface
/26	140.24.7.0	----------	m0
/26	140.24.7.64	----------	m1
/26	140.24.7.128	----------	m2
/26	140.24.7.192	----------	m3
/0	0.0.0.0	Default	m4

Routing table for R1

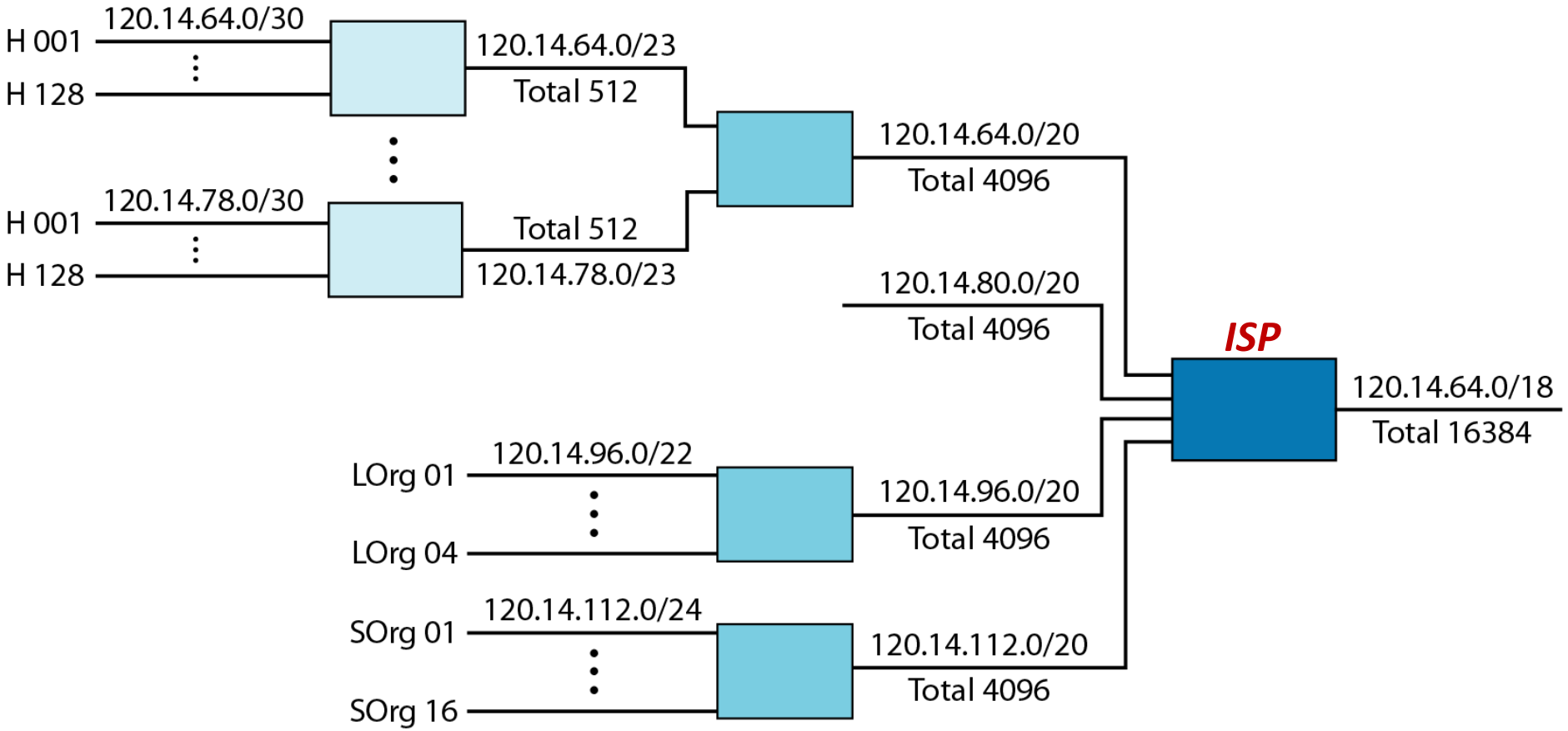
Mask	Network address	Next-hop address	Interface
/24	140.24.7.0	----------	m0
/0	0.0.0.0	Default	m1

Routing table for R2

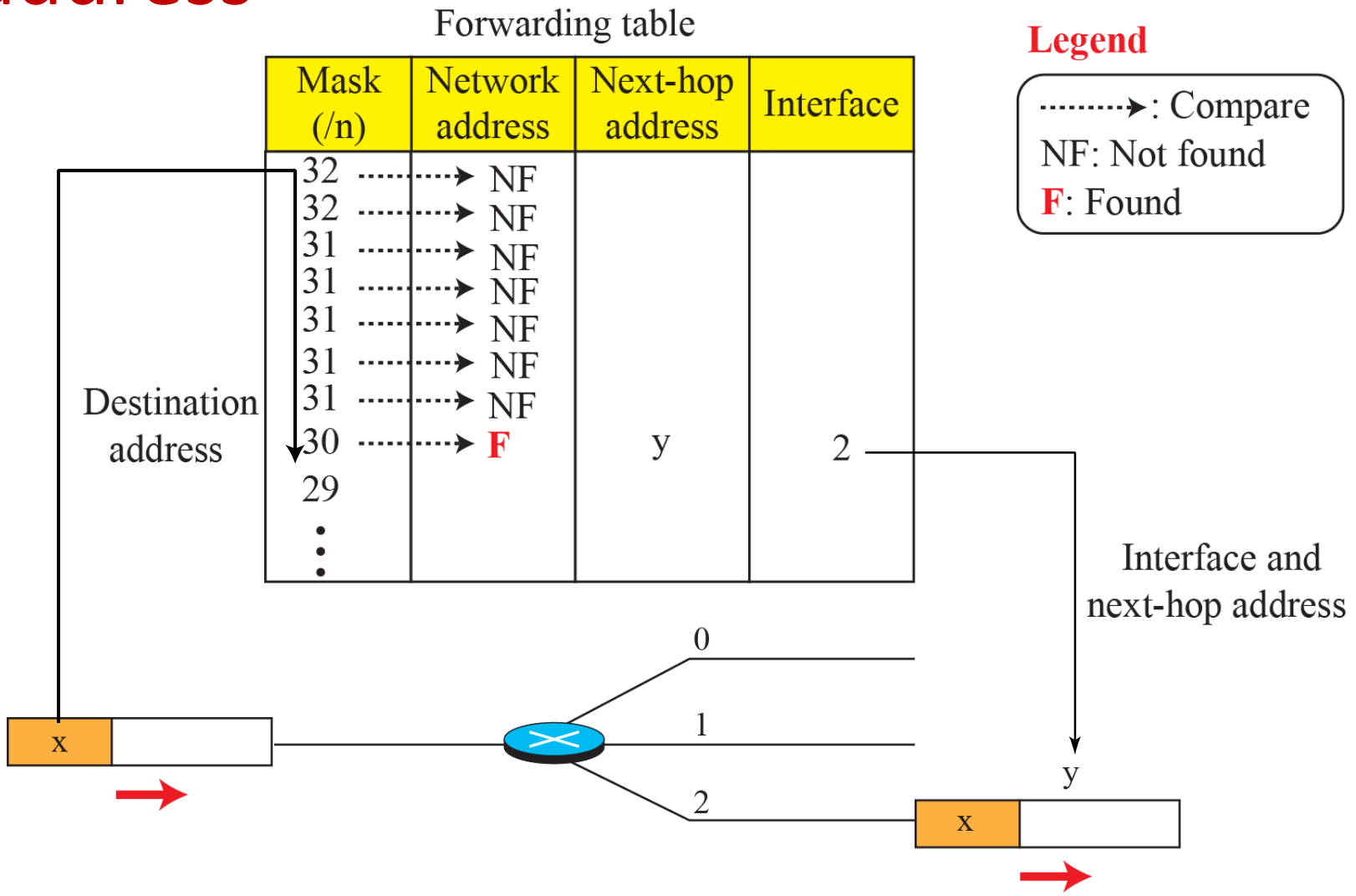
Forwarding: Longest mask matching



Forwarding: Hierarchical routing

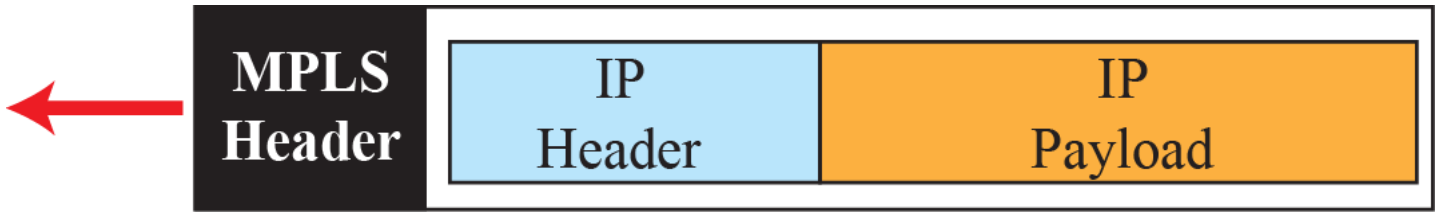


Forwarding based on destination address

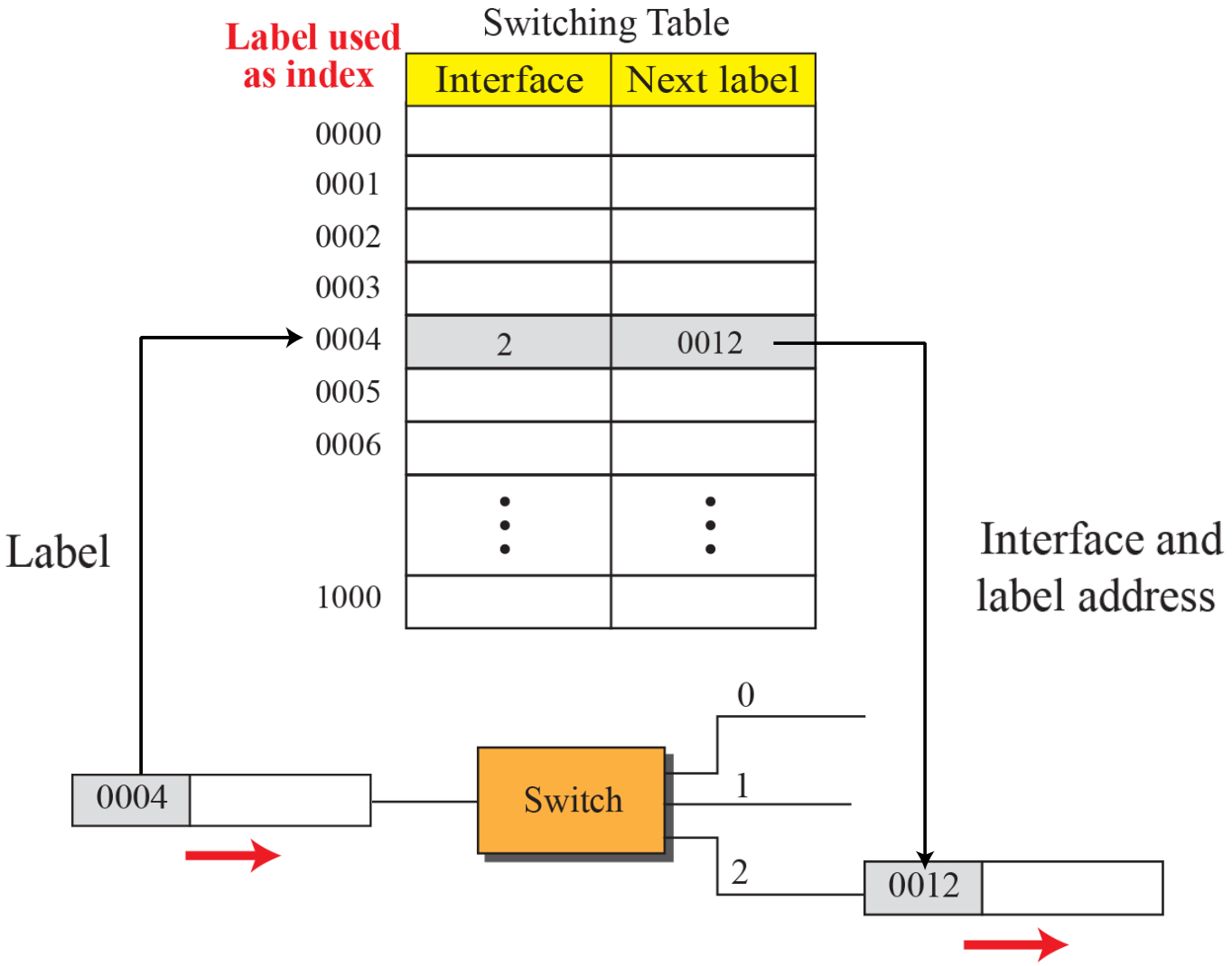


Label Switching

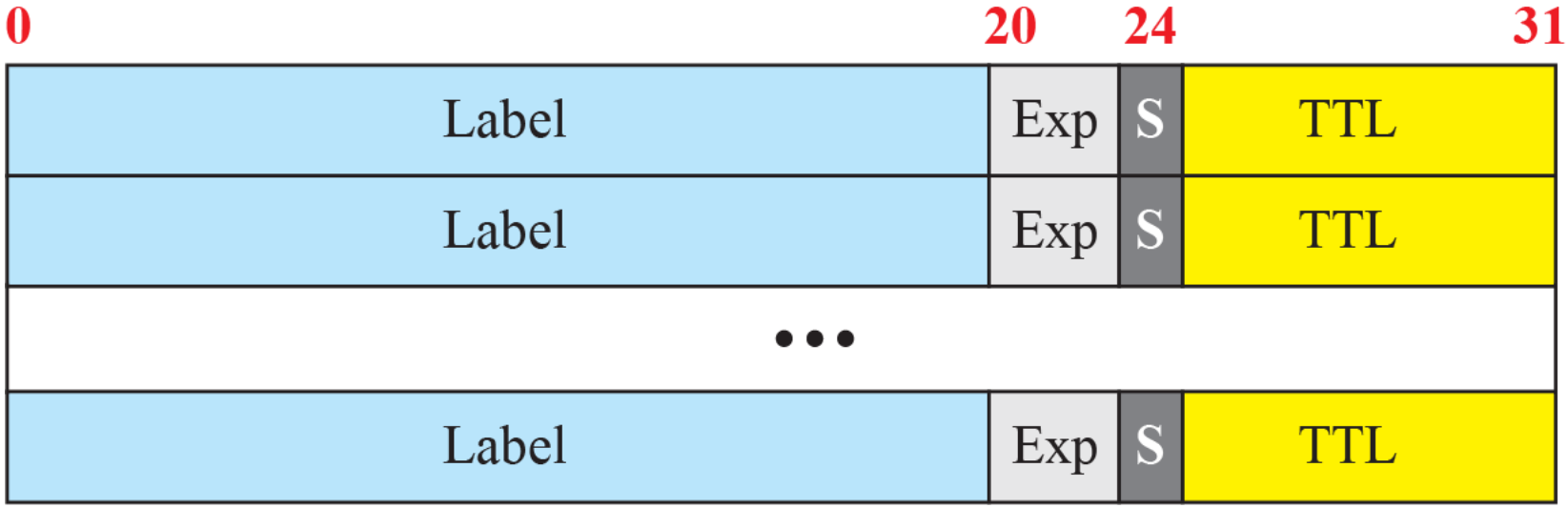
- Switching is more efficient than routing
- Create one path instead of routing/forwarding each individual packet hop by hop
  - Switching still hop by hop
  - Compare ATM switching
- MPLS (Multi-Protocol Lable Switching)



Forwarding based on label



MPLS header made of a stack of labels

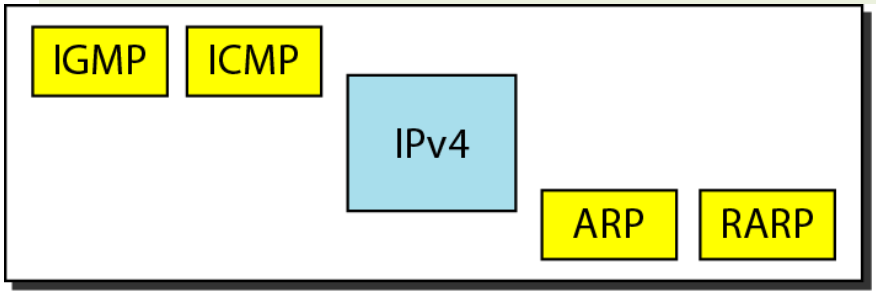


- Ex: One label for outside an organisation
- Ex: One label for inside a organisation
- Compare hierarchical routing

Internet Protocol

IPv4

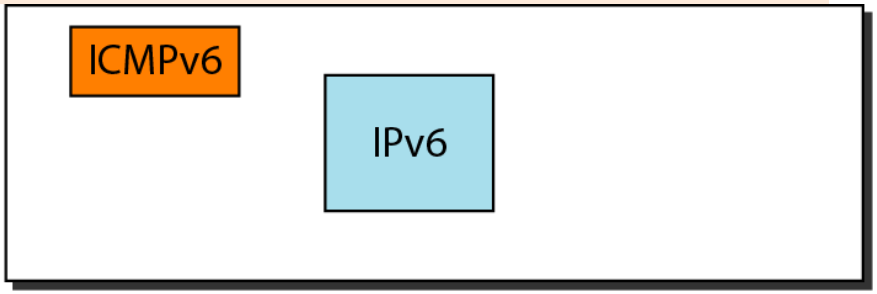
- Addressing scheme
  - Hierarchy
  - Configuration
  - Lookup
- Datagram format



Network layer in version 4

IPv6

- Larger address space
- Better header format
  - Extendible
  - More secure
- Support for QoS

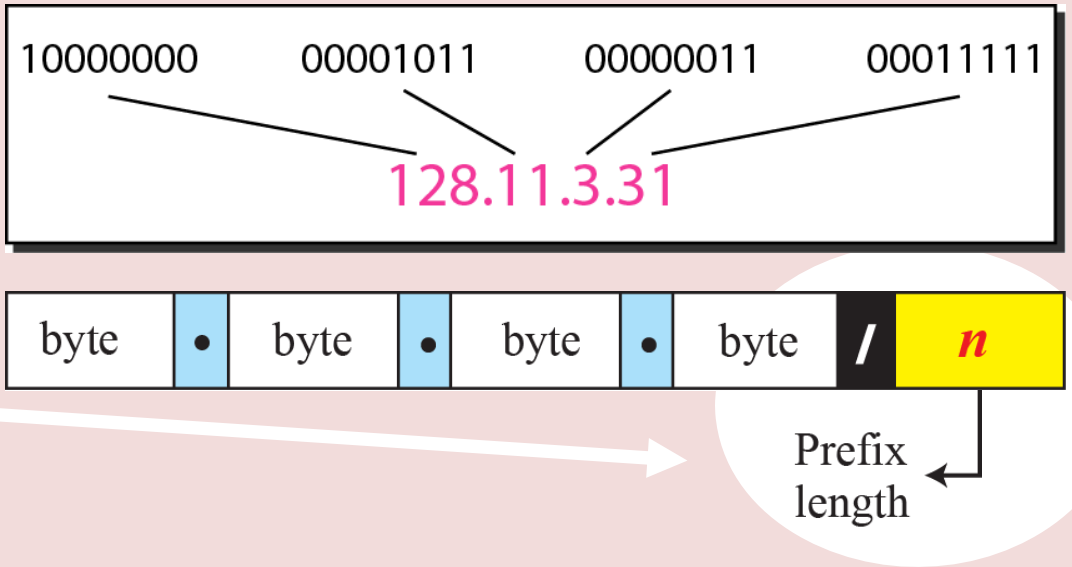


Network layer in version 6

IPv4 addresses

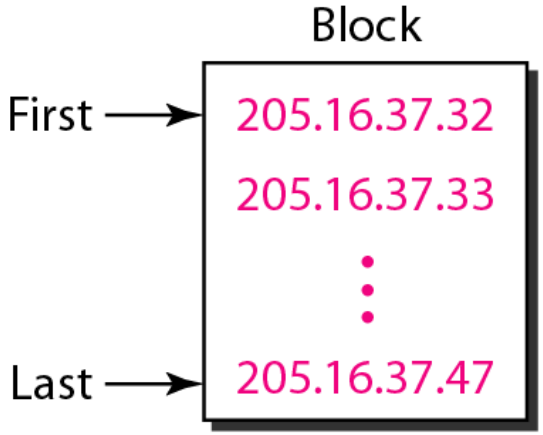
- 32 bits = 4 bytes
- $2^{32} = (2^8)^4 = 256^4 = 4\ 294\ 967\ 296$
- Classful vs. classless hierarchy

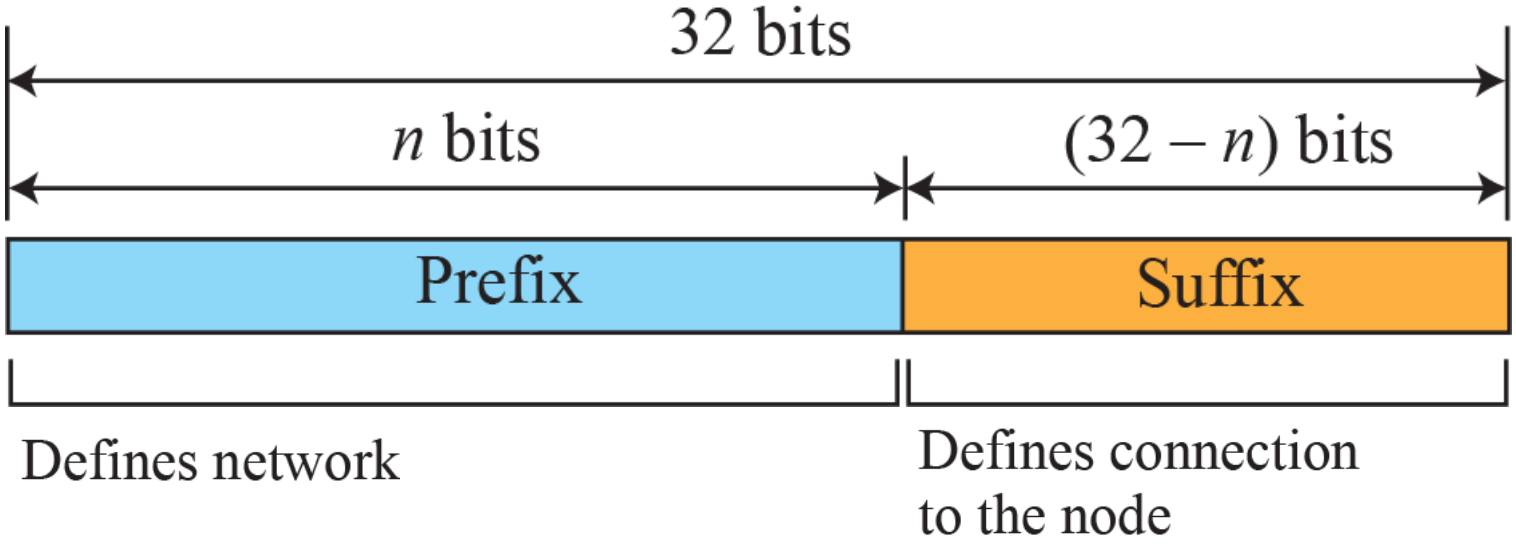
- Notations
  - Dotted decimal
  - Slash (CIDR)



Classless addressing

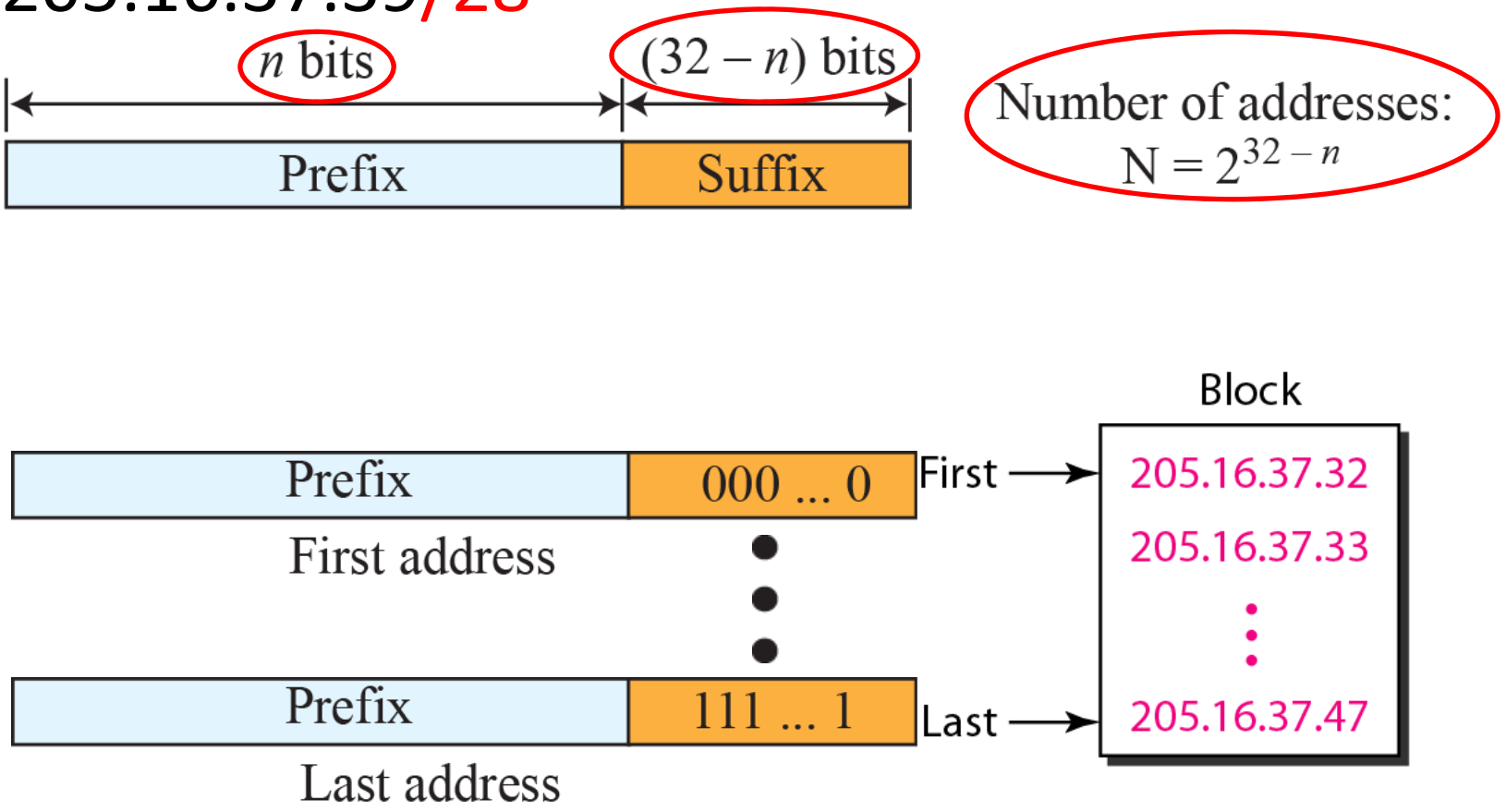
- Addresses in blocks
  - Block size power of 2
  - $N = 2^{32-n}$





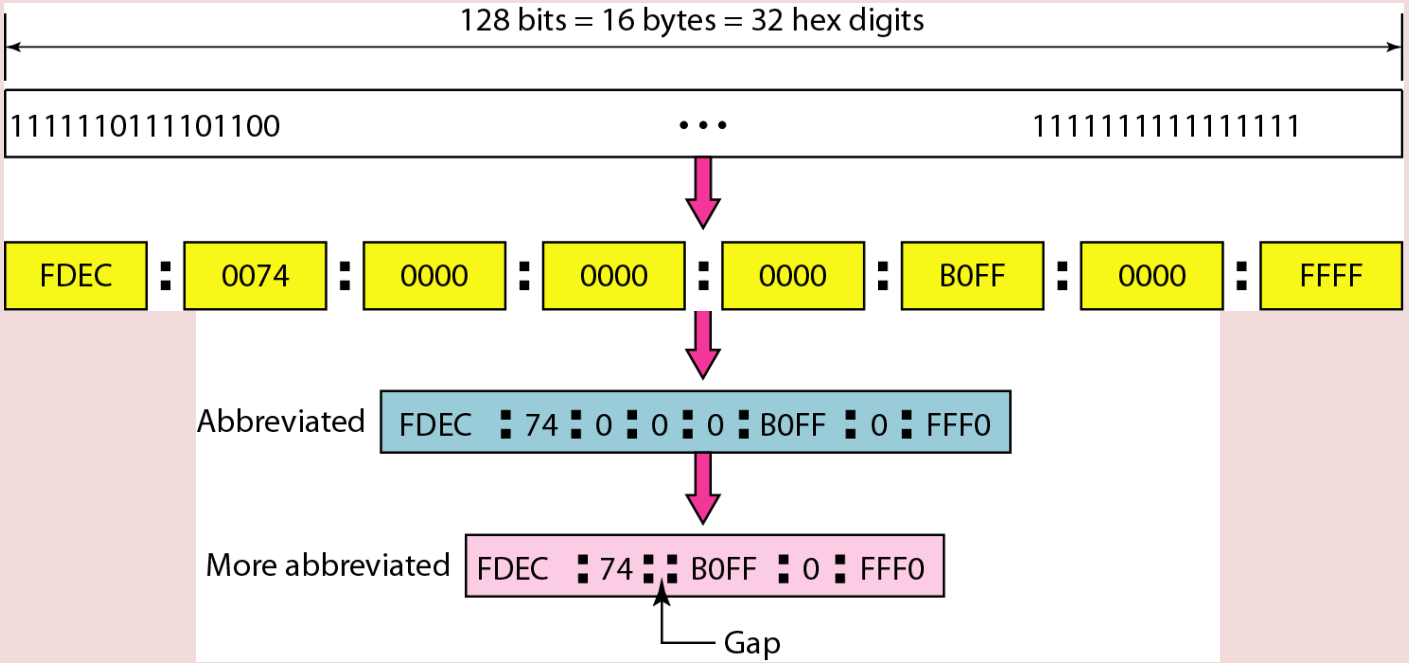
Example: Classless addressing

- 205.16.37.39/28



IPv6 addresses

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

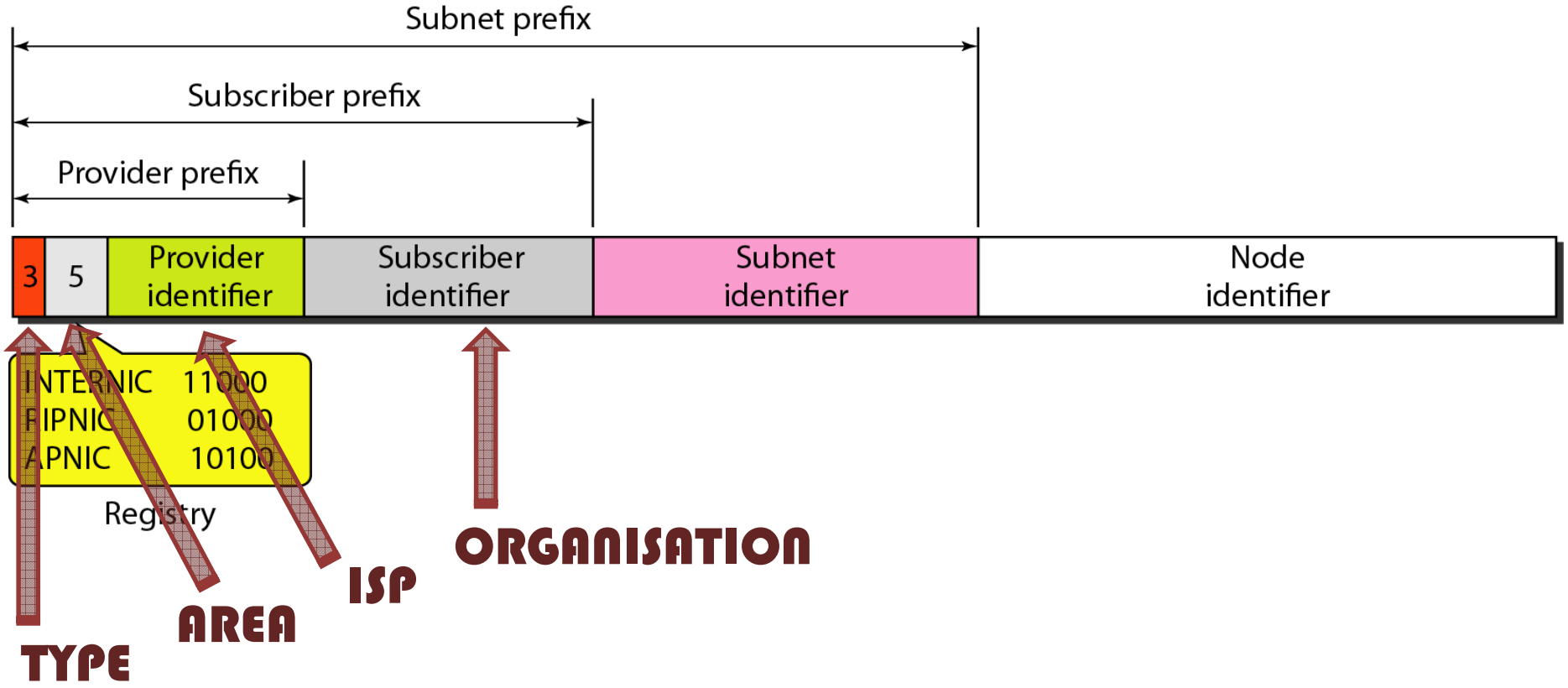


Prefixes for assigned IPv6 addresses

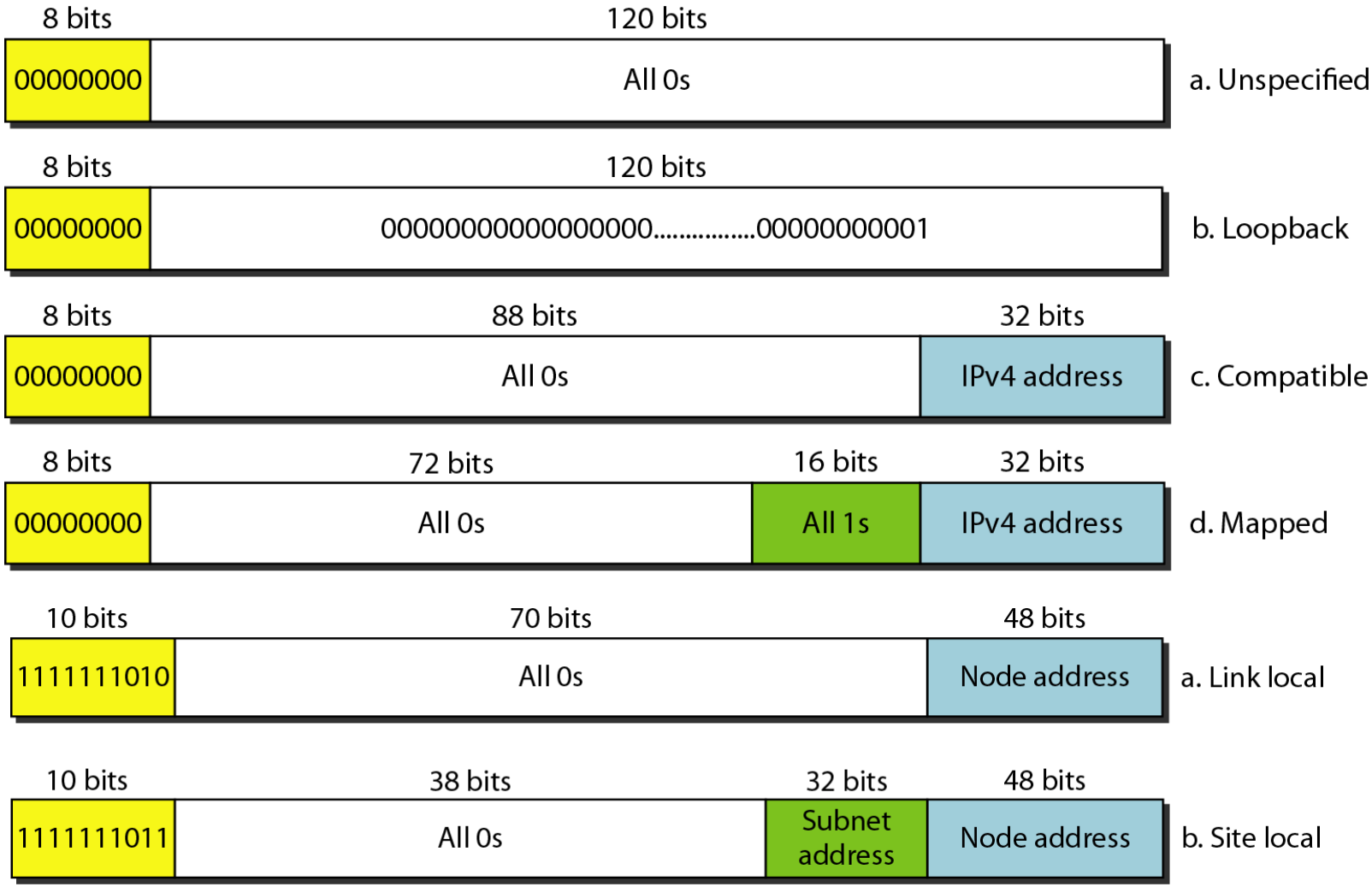
Block prefix	*CIDR*	*Block assignment*	*Fraction*
0000 0000	0000::/8	Special addresses	1/256
001	**2000::/3**	**Global unicast**	**1/8**
1111 110	FC00::/7	Unique local unicast	1/128
1111 1110 10	FE80::/10	Link local addresses	1/1024
1111 1111	FF00::/8	Multicast addresses	1/256

Global unicast addresses

- Identify individual computers

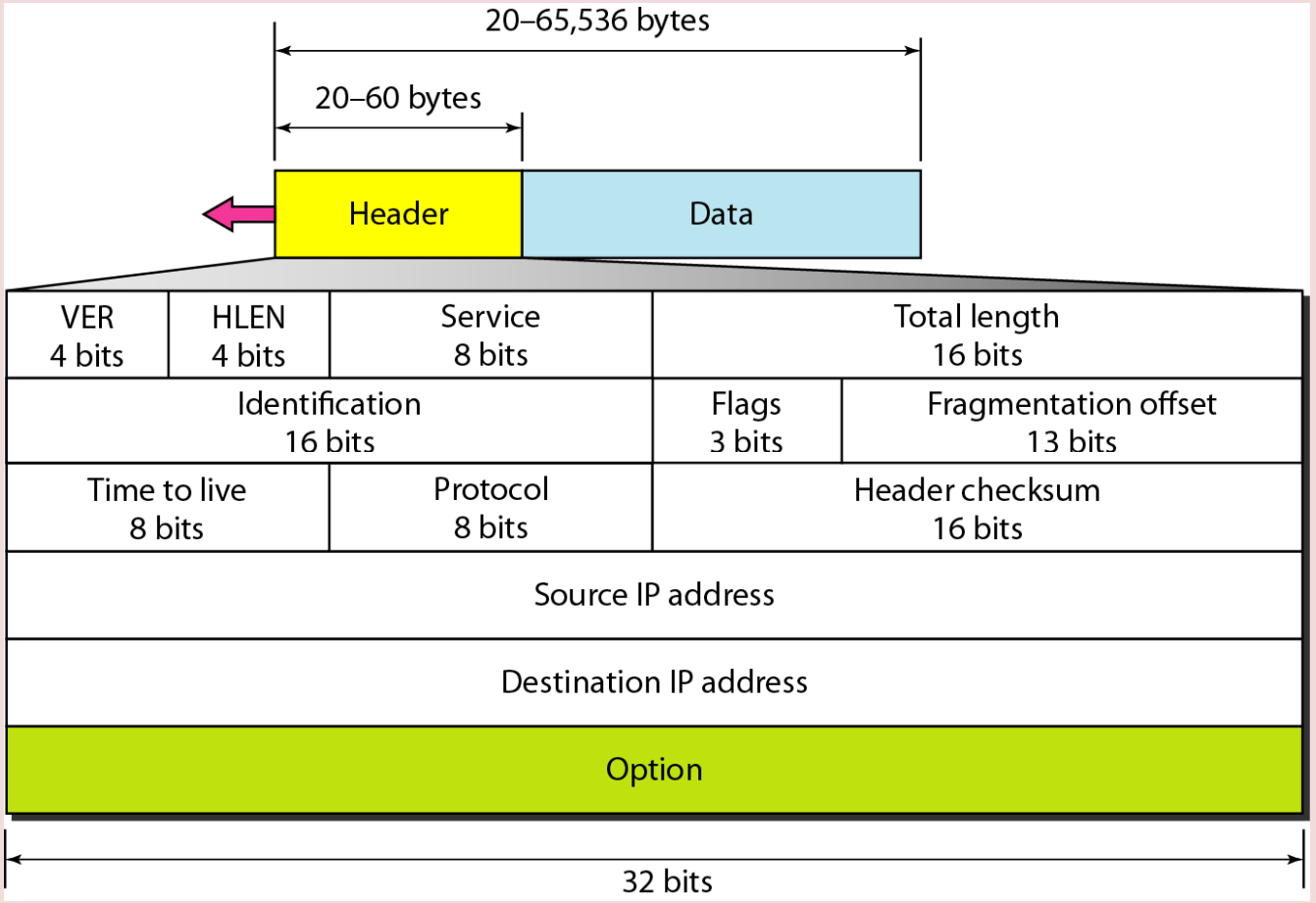


A few special IPv6 addresses

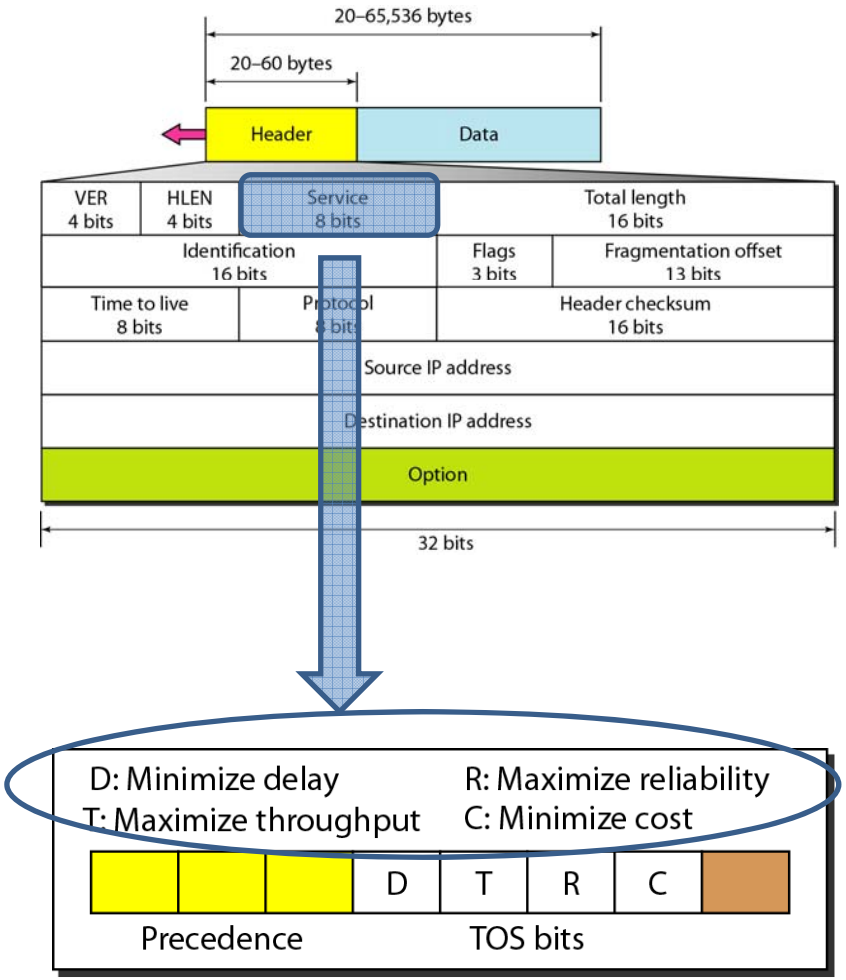


AUTOCONFIG

IPv4 datagram

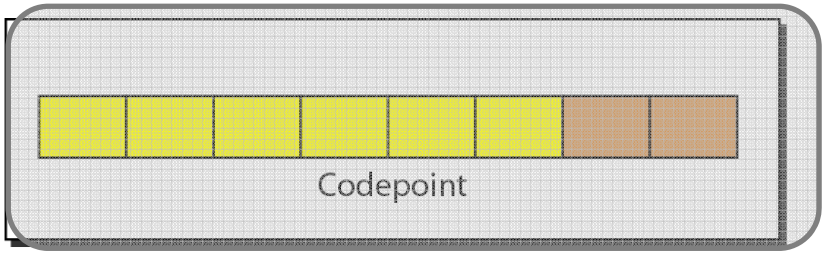


Service type field



Service type

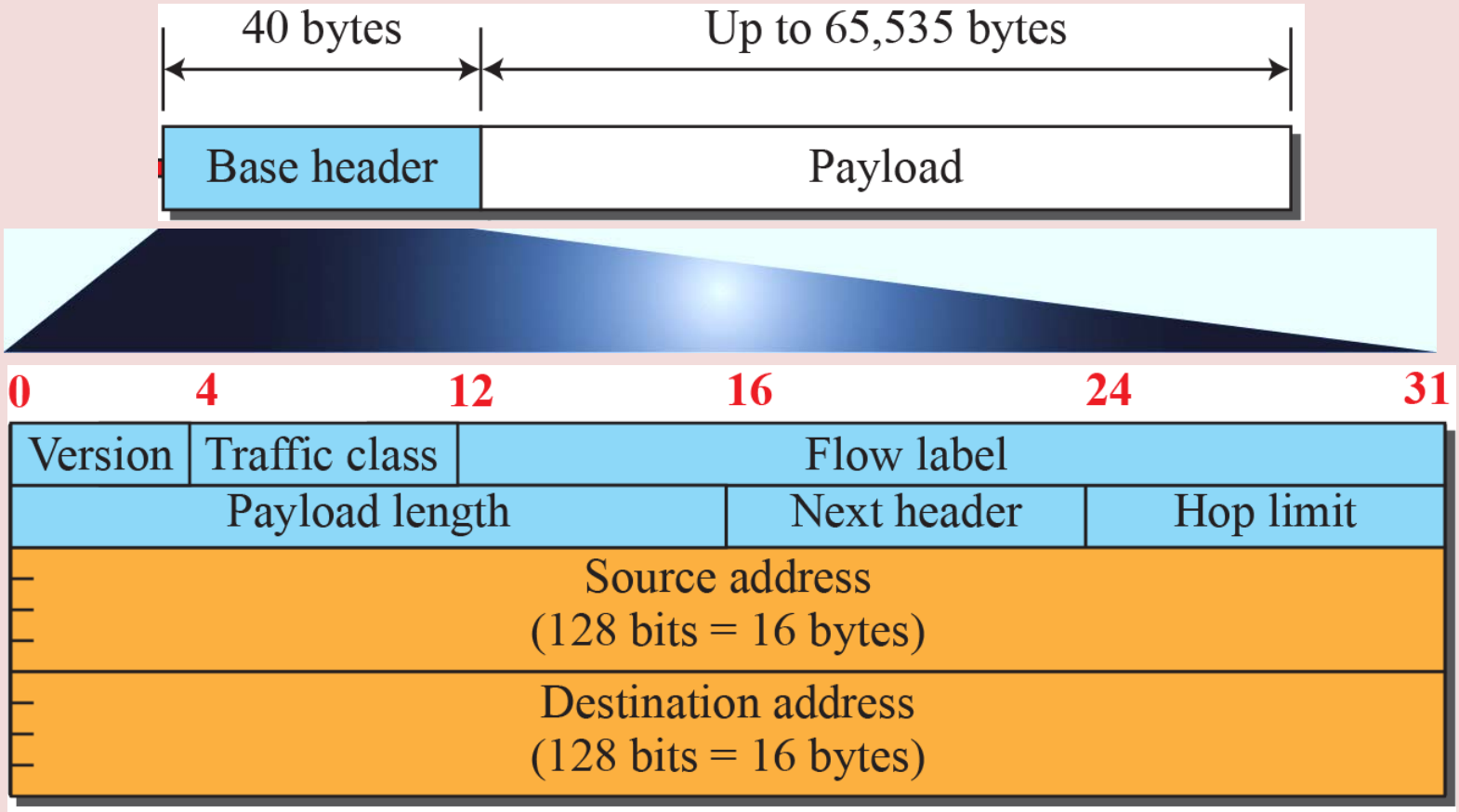
Protocol	*TOS Bits*	*Description*
ICMP	0000	Normal
BOOTP	0000	Normal
NNTP	0001	Minimize cost
IGP	0010	Maximize reliability
SNMP	0010	Maximize reliability
TELNET	1000	Minimize delay
FTP (data)	0100	Maximize throughput
FTP (control)	1000	Minimize delay
TFTP	1000	Minimize delay
SMTP (command)	1000	Minimize delay
SMTP (data)	0100	Maximize throughput
DNS (UDP query)	1000	Minimize delay
DNS (TCP query)	0000	Normal
DNS (zone)	0100	Maximize throughput



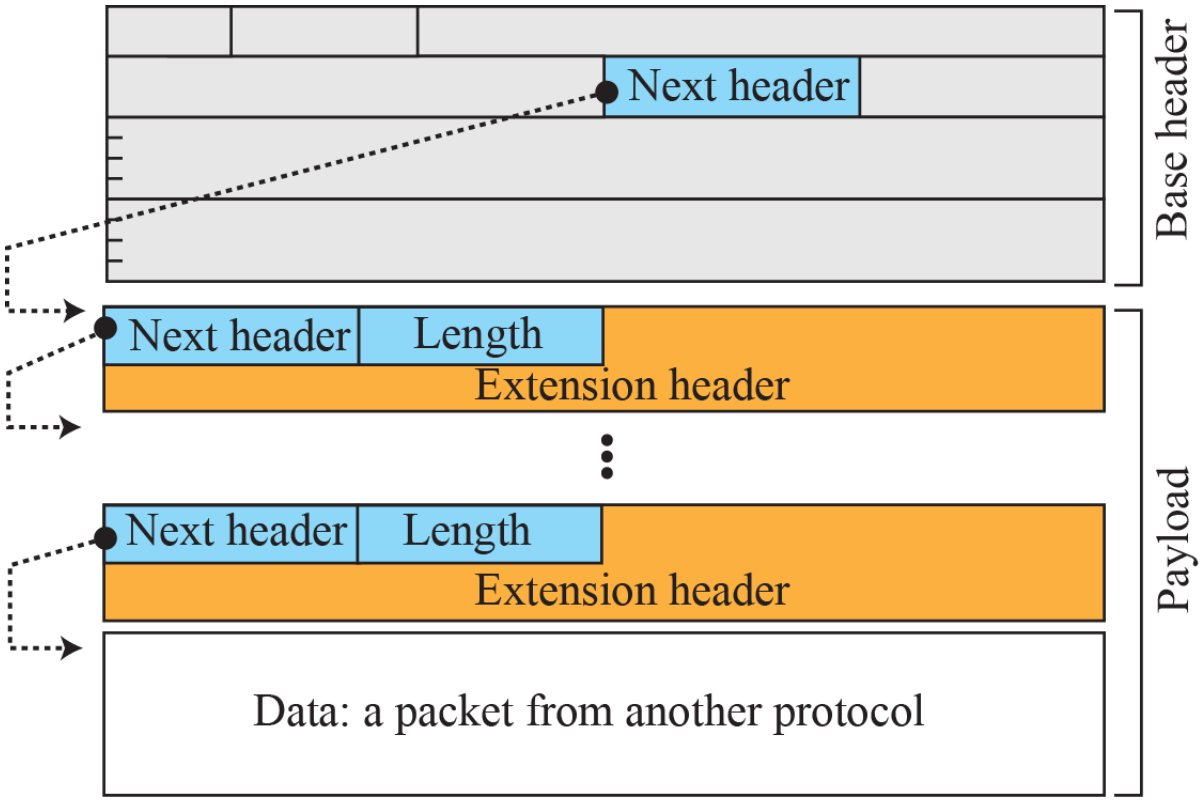
Differentiated services

IPv6 datagram

- Simpler base header, flexible for extensions



IPv6 extension headers



Some next-header codes

00: Hop-by-hop option
02: ICMPv6
06: TCP
17: UDP
43: Source-routing option
44: Fragmentation option
50: Encrypted security payload
51:Authentication header
59: Null (no next header)
60: Destination option

Traffic Classes → Packet priorities

- 0 .. 7
  - Congestion controlled

Priority	*Meaning*
0	No specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

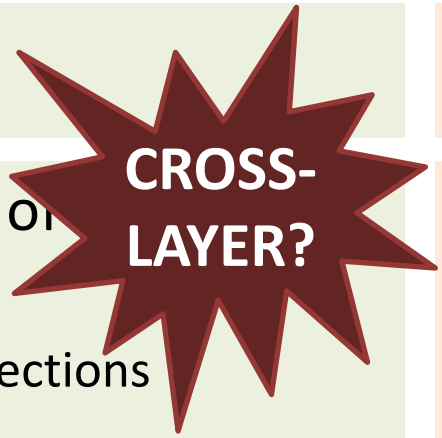
- 8 .. 15
  - Non-congestion controlled

Priority	*Meaning*
8	Data with greatest redundancy
. . .	. . .
15	Data with least redundancy

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!

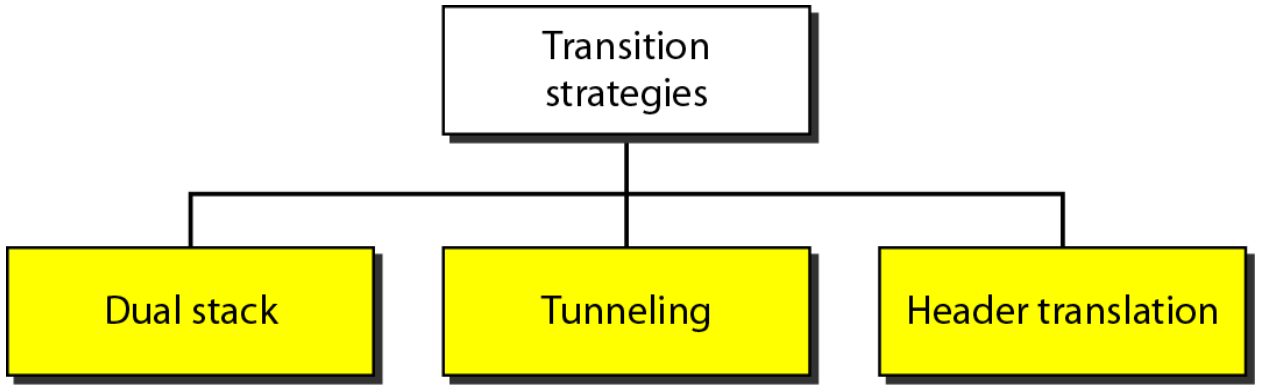


Traffic class

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

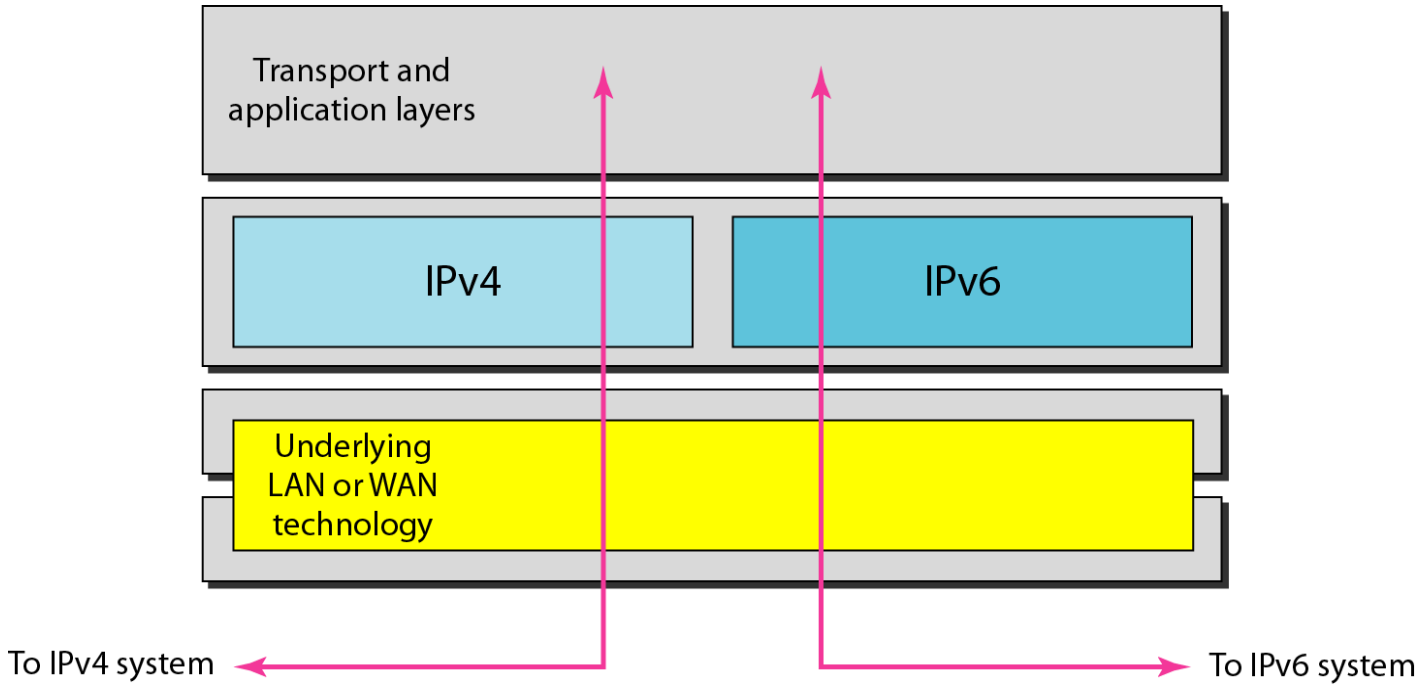
Transition: IPv4 → IPv6

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



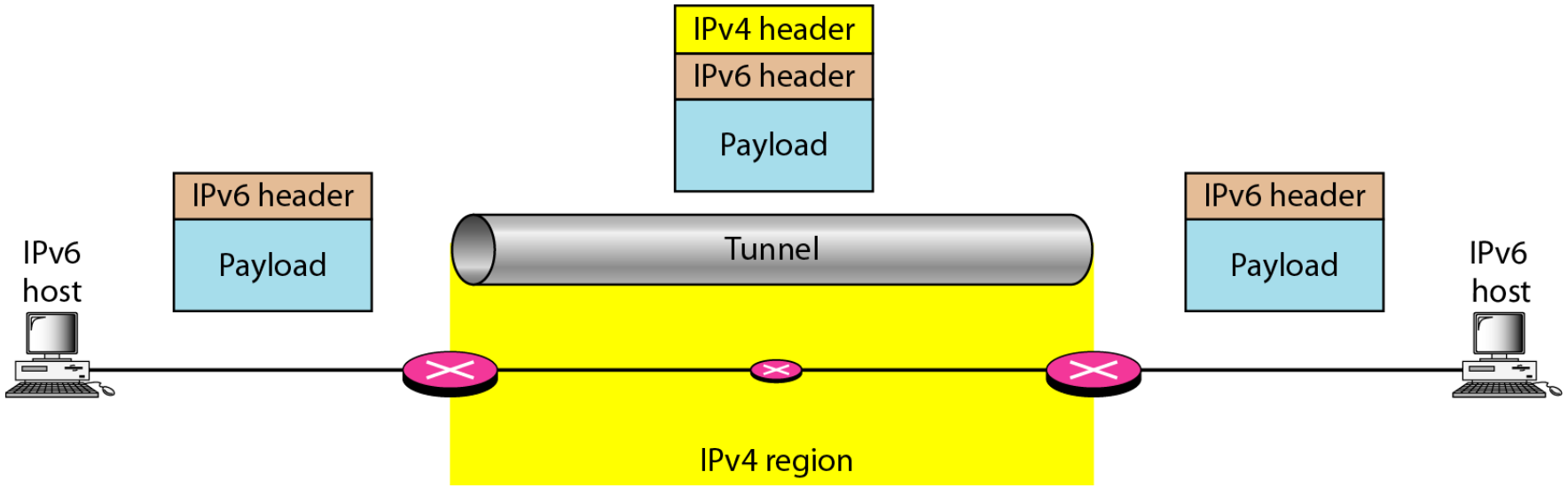
Transition: (1) Dual stack

- Decision based on destination IP



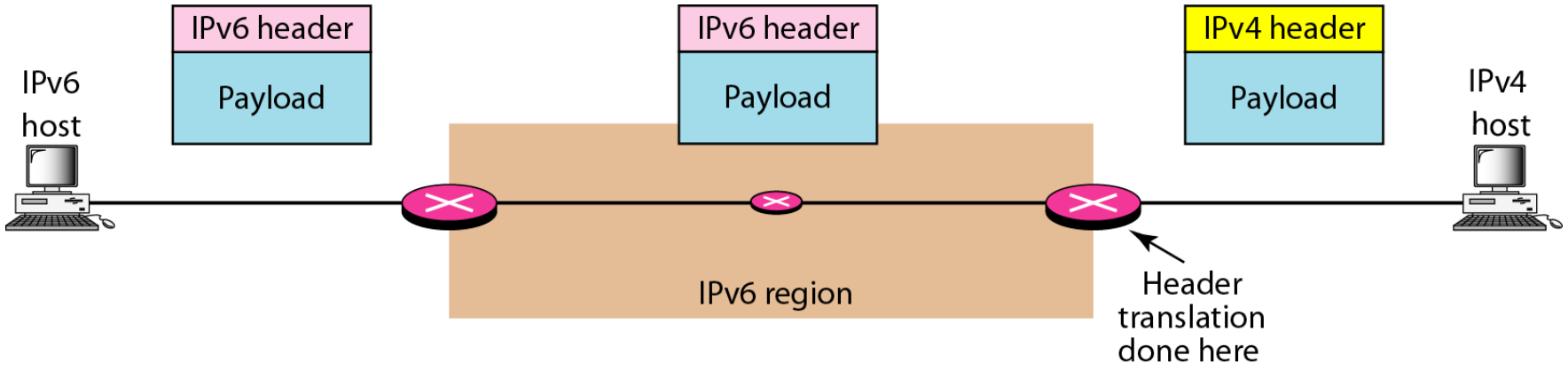
Transition: (2) Tunneling

- A few IPv6 routers



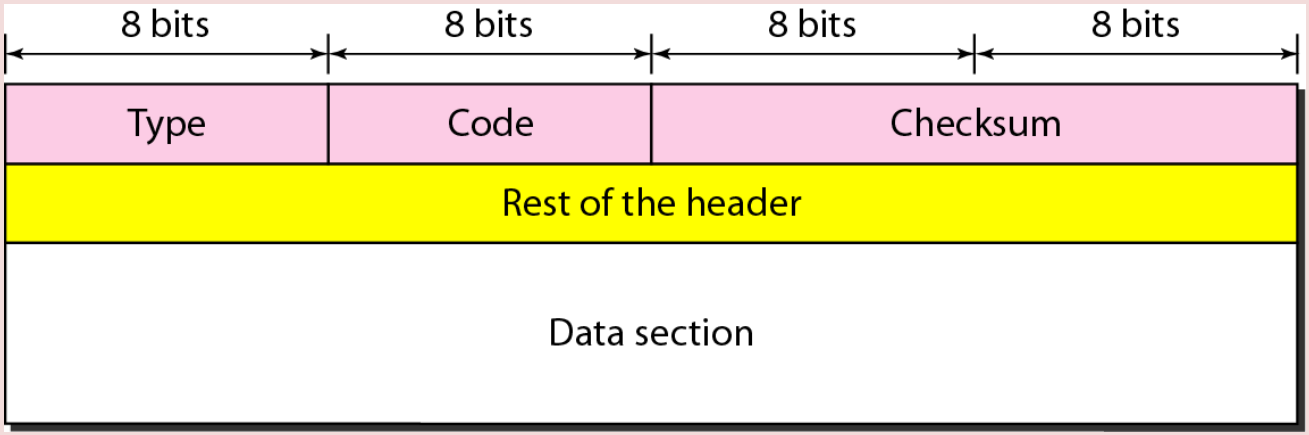
Transition: (3) Header translation

- A few IPv4 routers

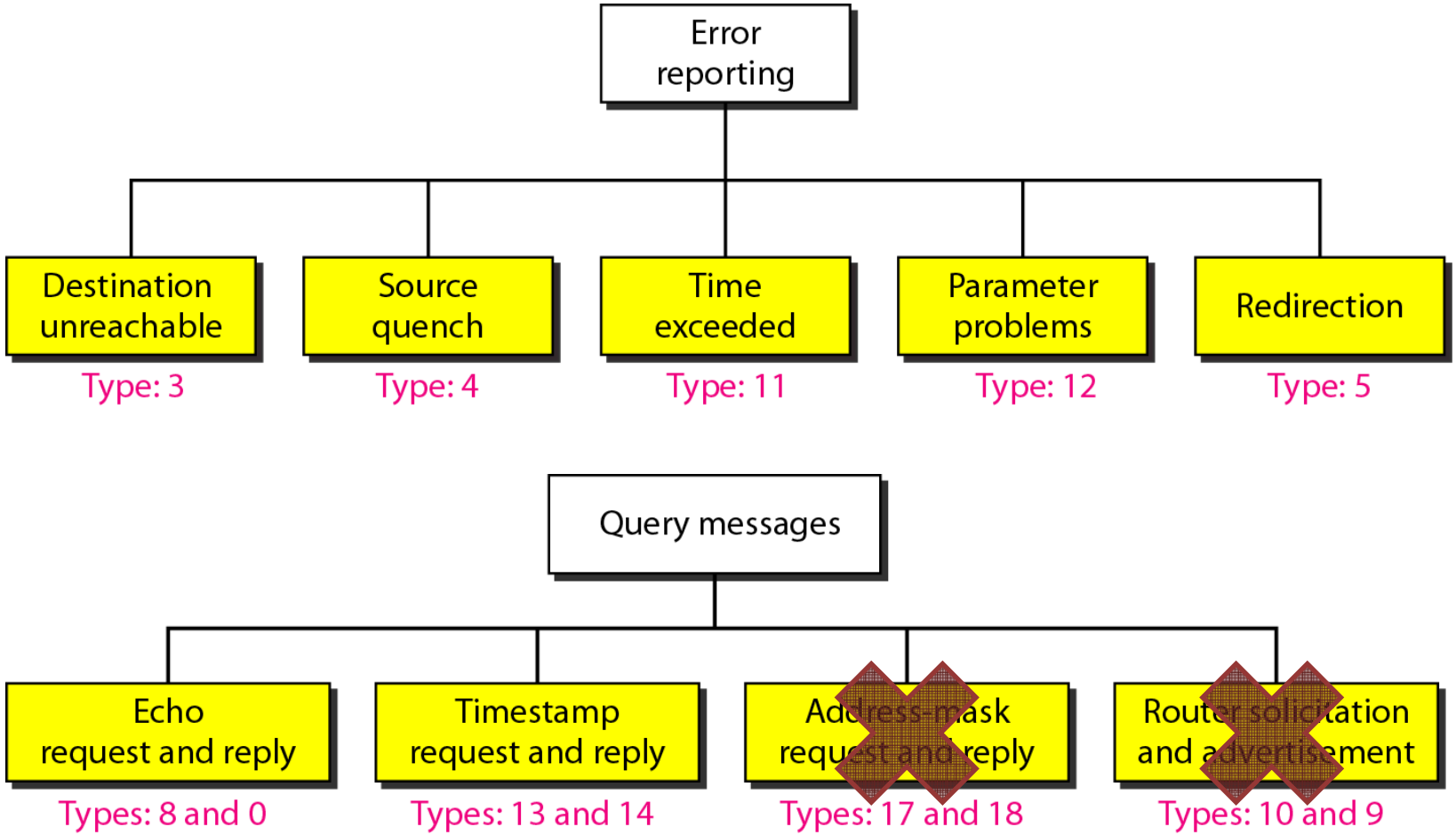


Internet Control Message Protocol

- ICMP
- Support protocol for IP
  - Error reporting
  - Query

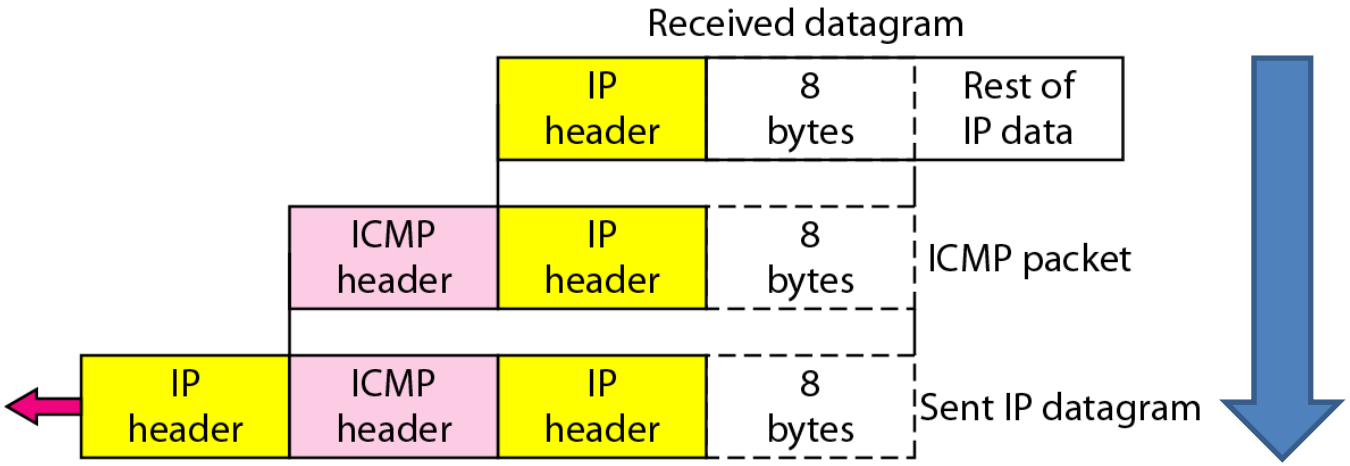


ICMPv4 message types

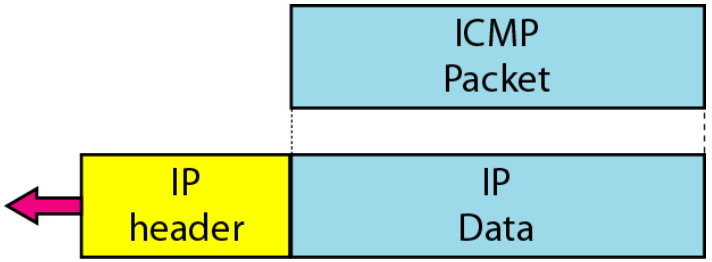


ICMP message formats

- Error reporting

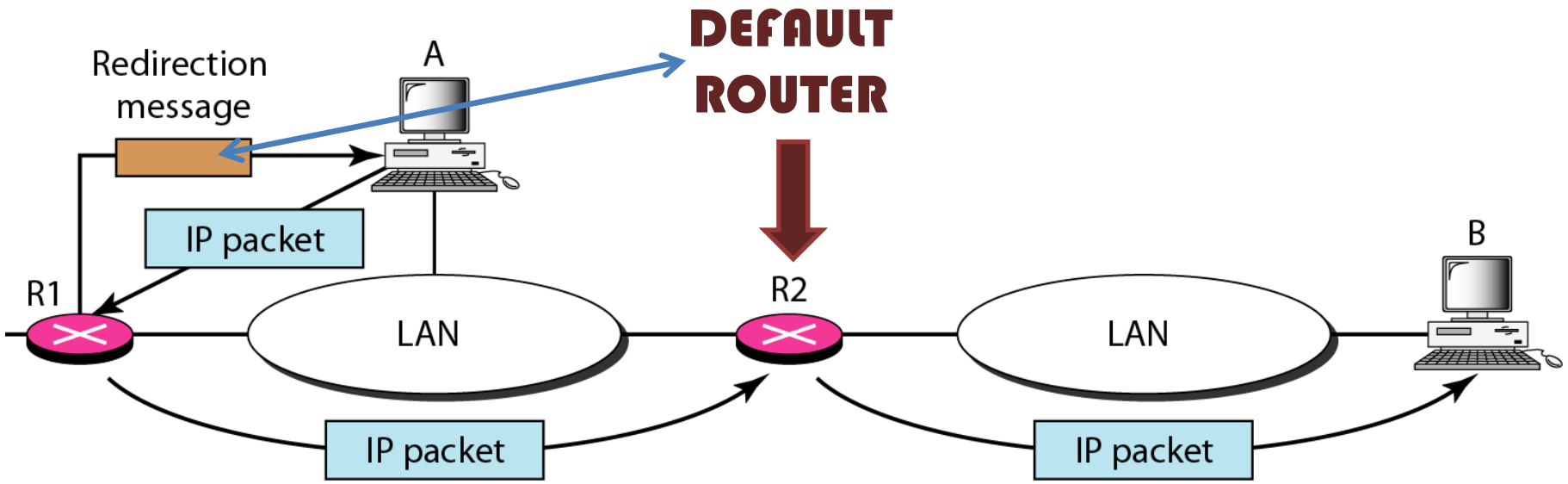


- Query messages



Redirection (error reporting type)

- Routing update for hosts
  - Security/reliability?

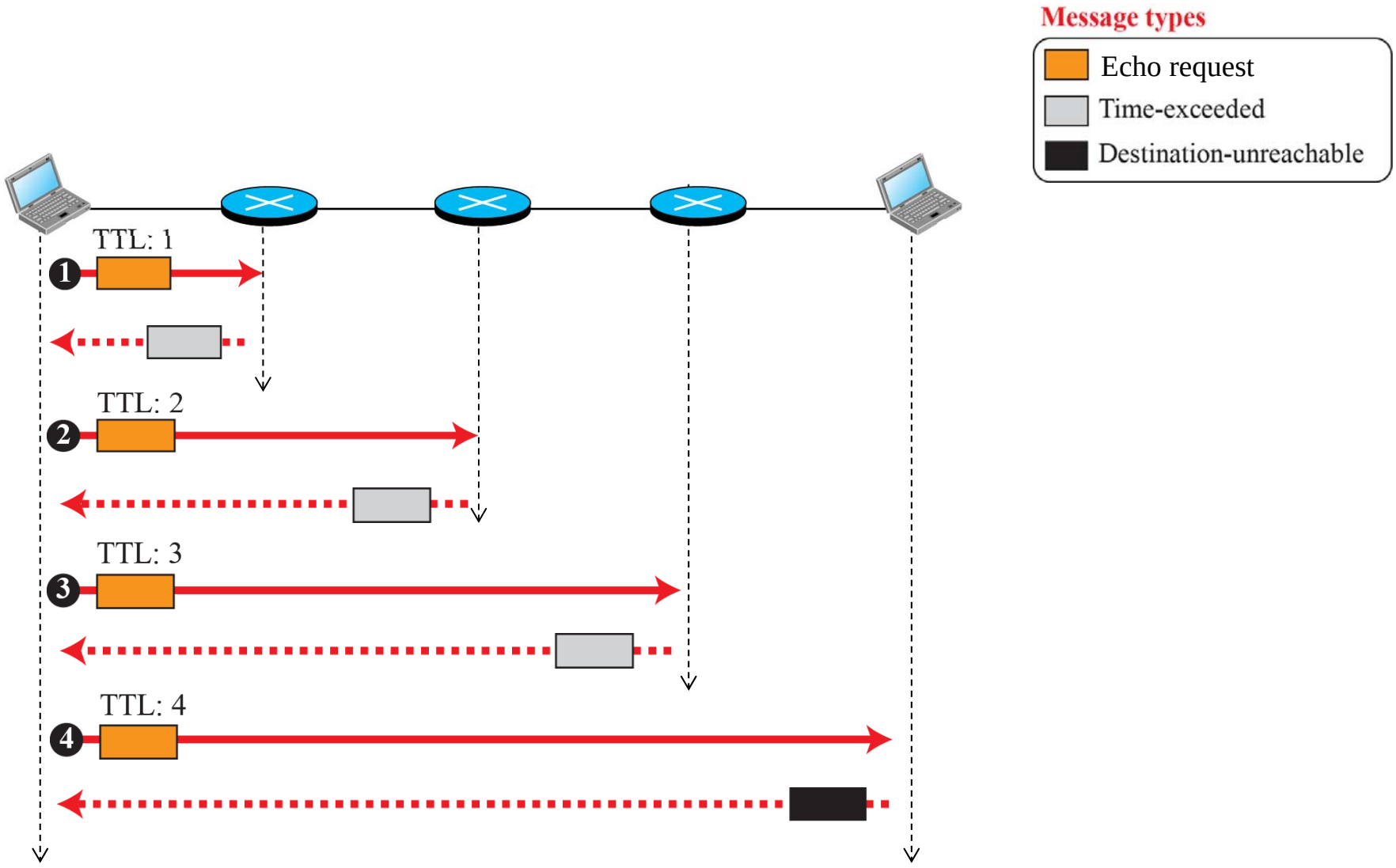


Echo request and reply (query type)

- Is my destination alive?

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

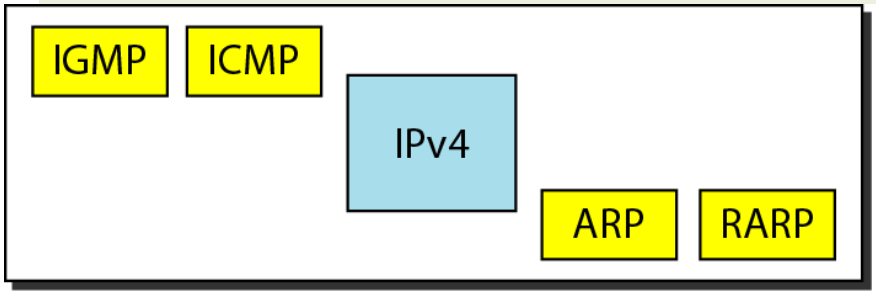
Traceroute


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

Changes to ICMP

ICMPv4

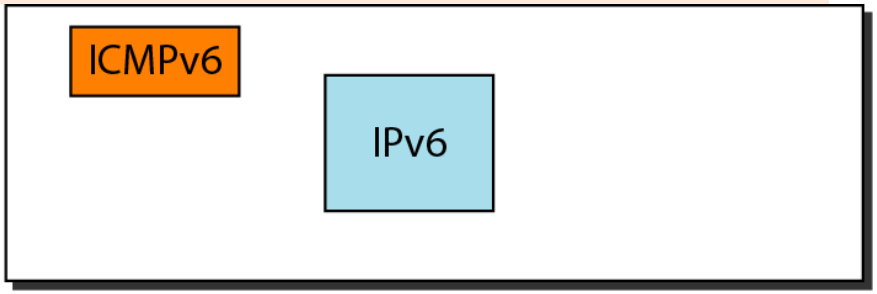
- Some unused functions



Network layer in version 4

ICMPv6

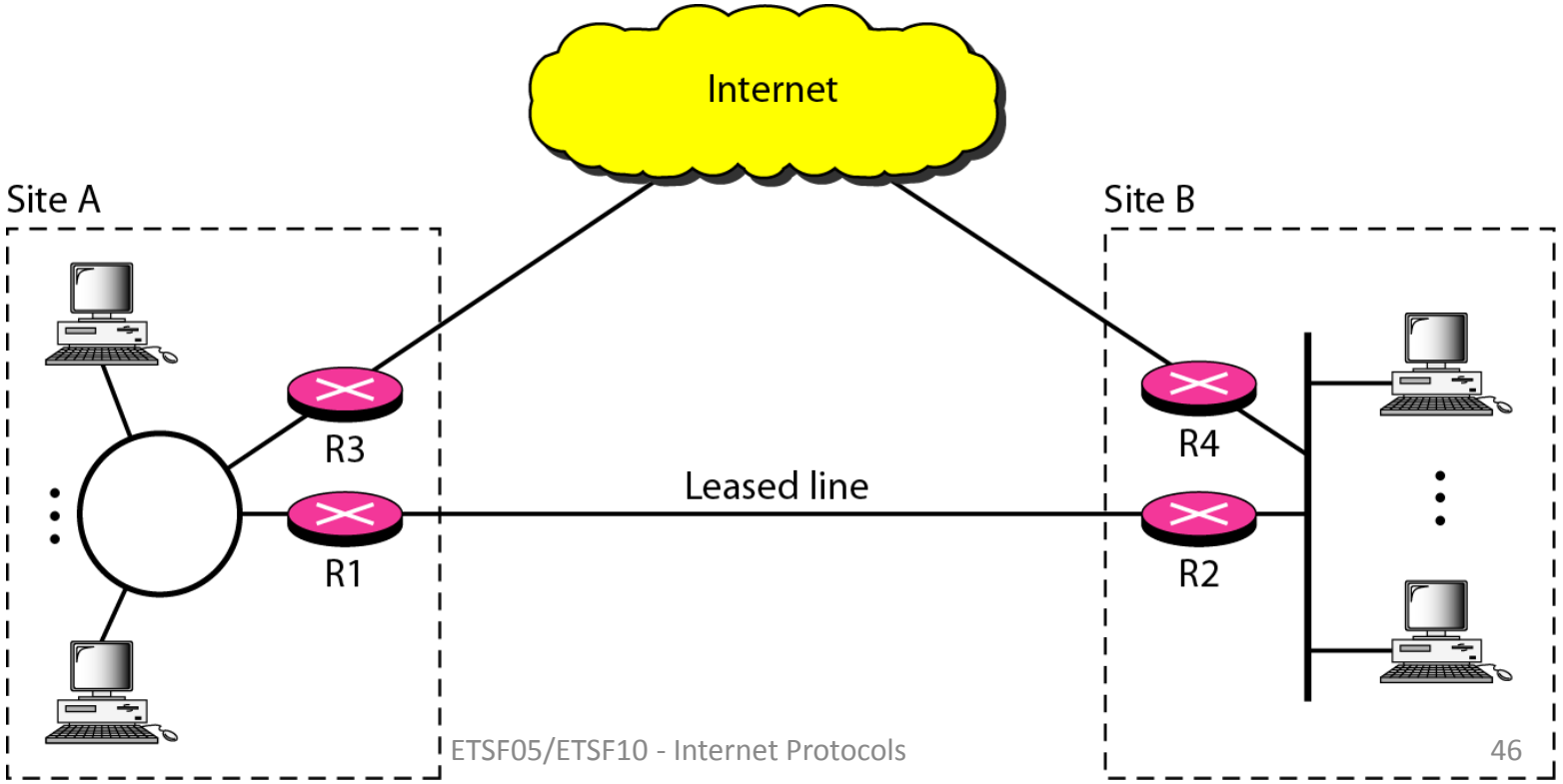
- Same principle
- Some new functions
- Convergence
- Suits IPv6 better



Network layer in version 6

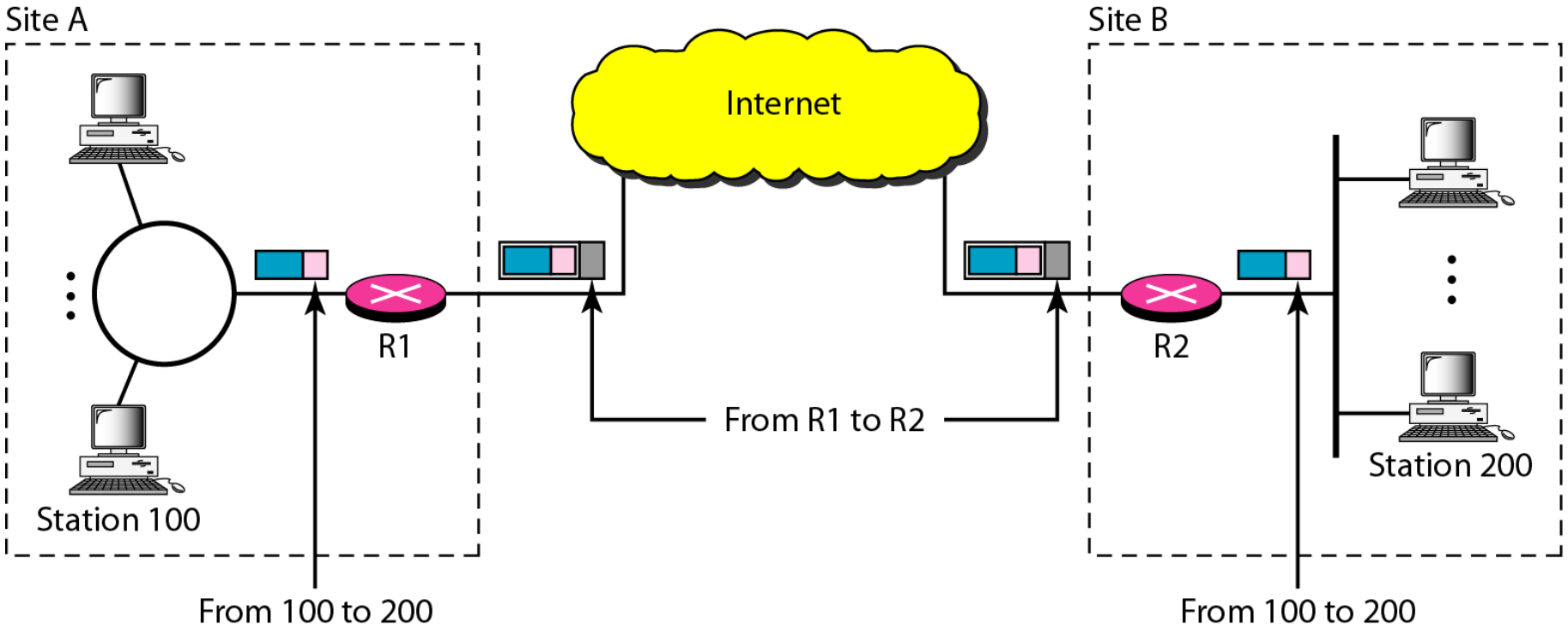
Virtual Private Network (VPN)

- Overlay network
- Alternative to a real private network



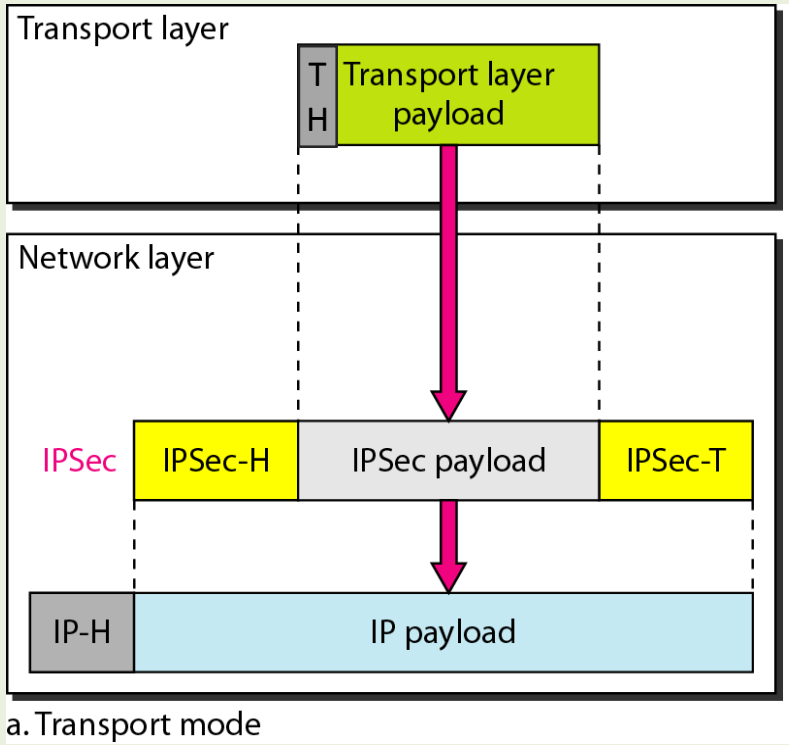
An example VPN

- IPSec between routers



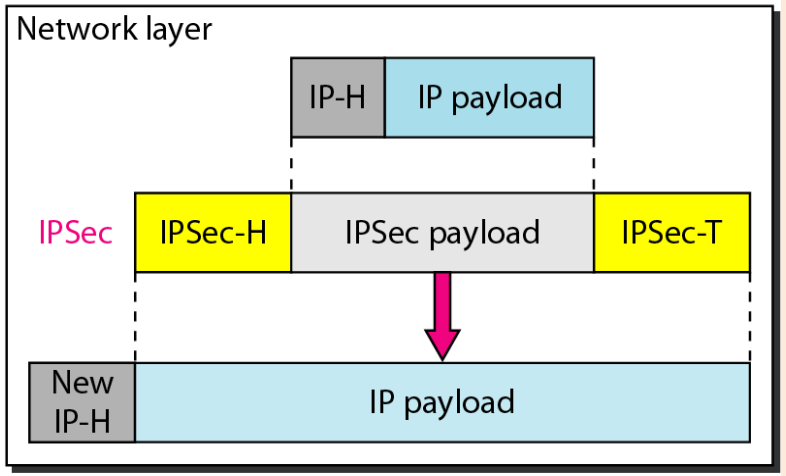
IPSec

Transport mode



a. Transport mode

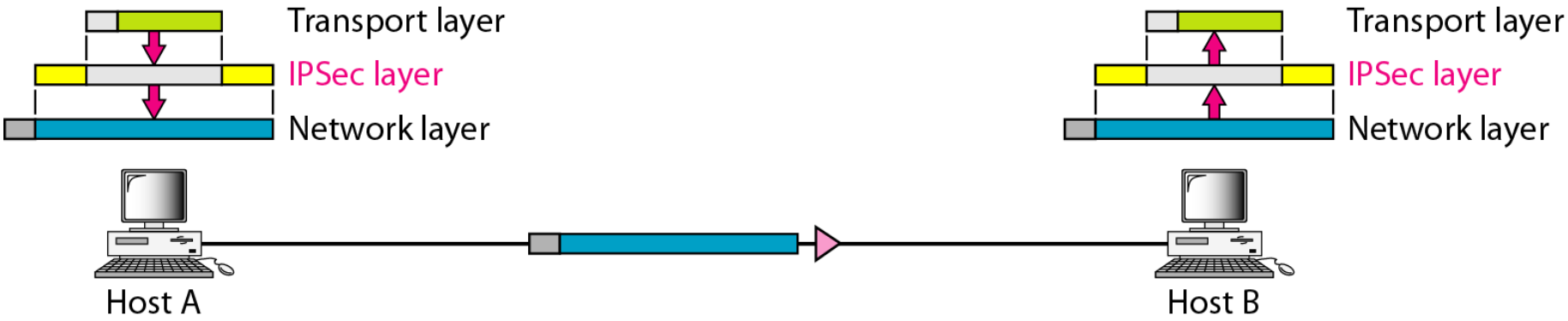
Tunnel mode



b. Tunnel mode

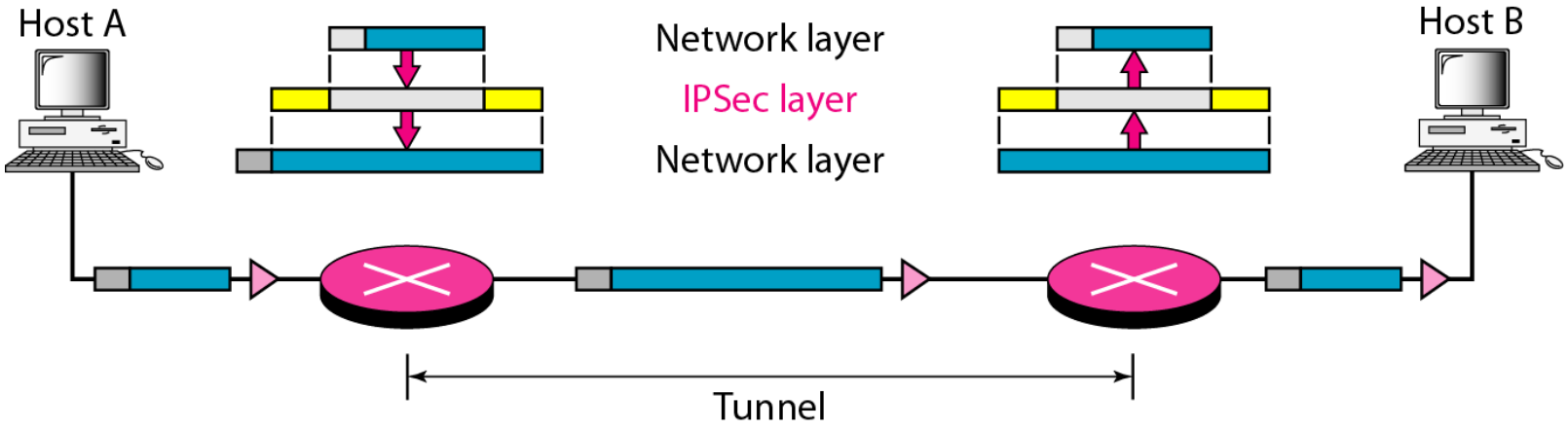
Transport mode in action

- Data protected
- Headers unprotected
  - Addresses fully visible

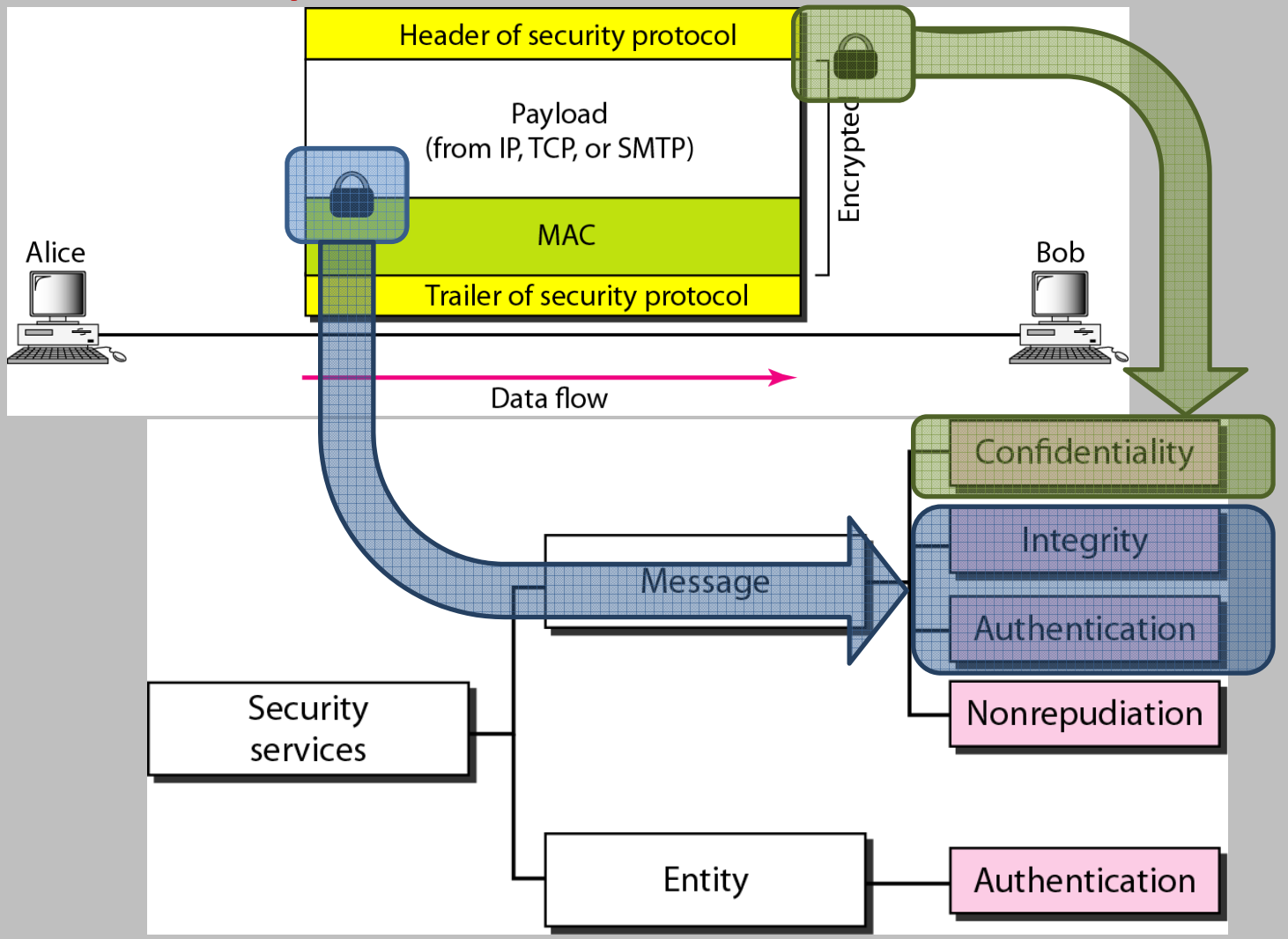


Tunnel mode in action

- 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