ETSF10 Part 3
Lect 1

IPv4 and IPv6, ICMP, RTP/RTCP, VoIP

Jens A Andersson

Electrical and Information Technology

IPv4

- Recap
- Some header fields
- MTU
- Fragmentation

Figure 20.2 *Network layer in an internetwork*

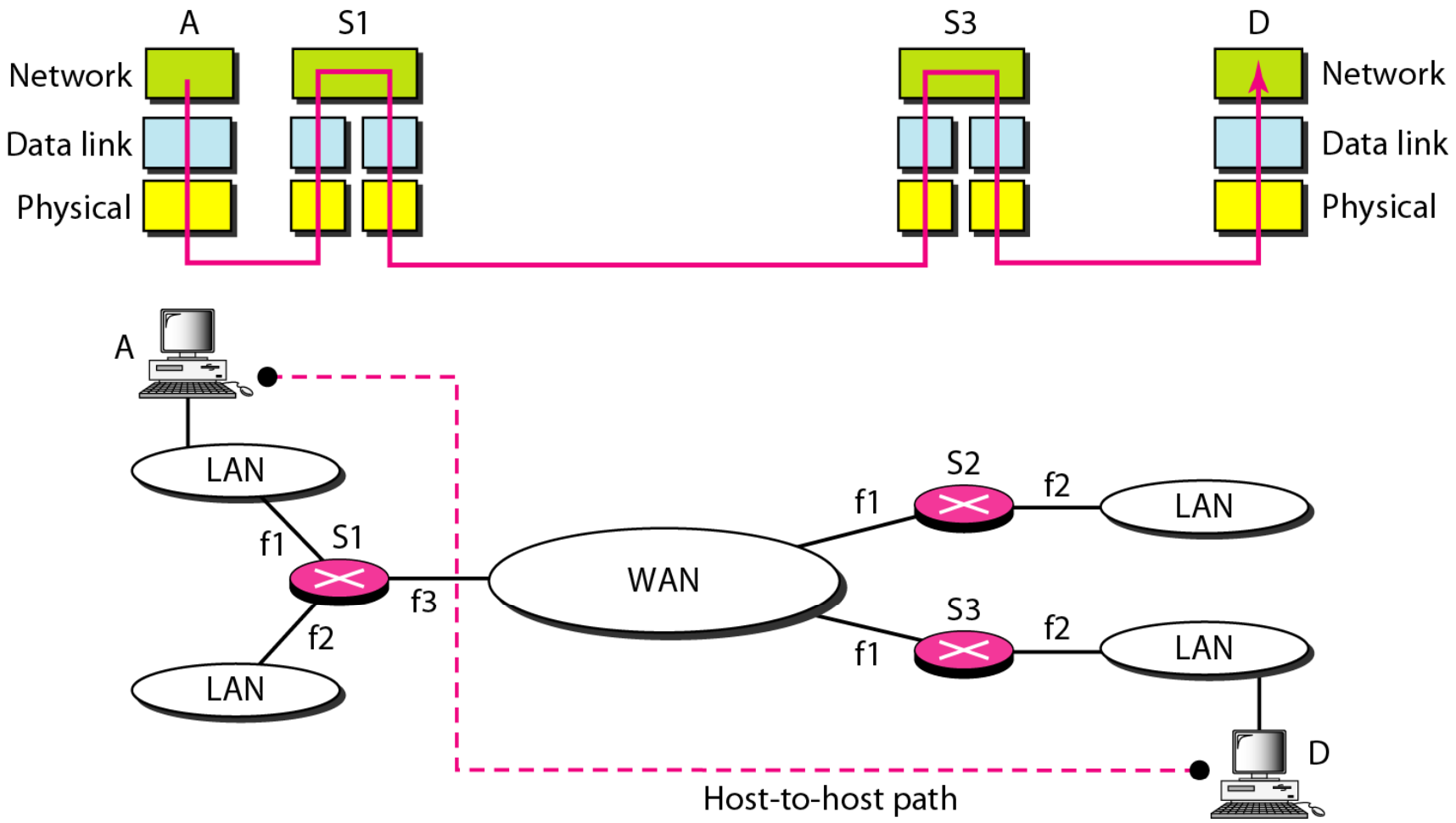


Figure 20.4 *Position of IPv4 in TCP/IP protocol suite*

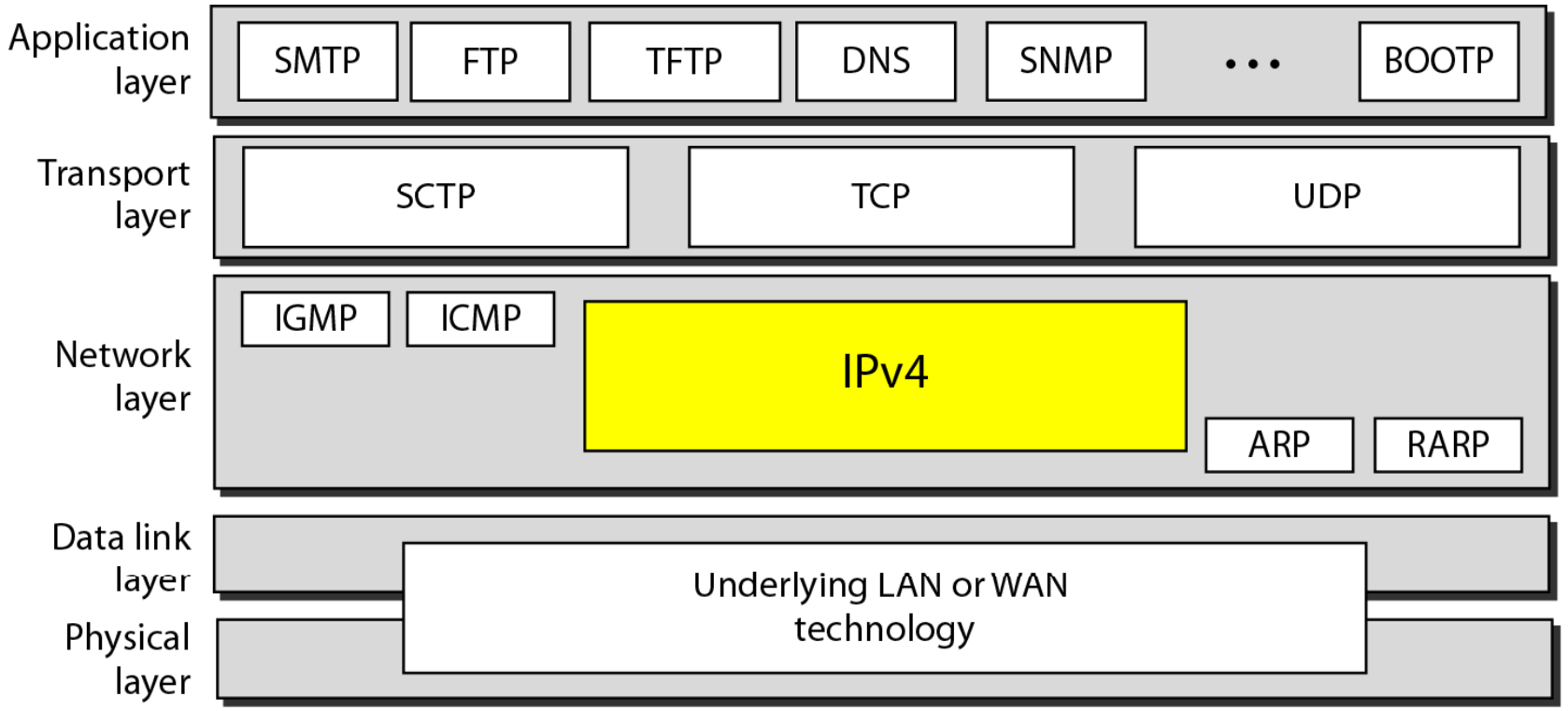


Figure 20.5 *IPv4 datagram format*

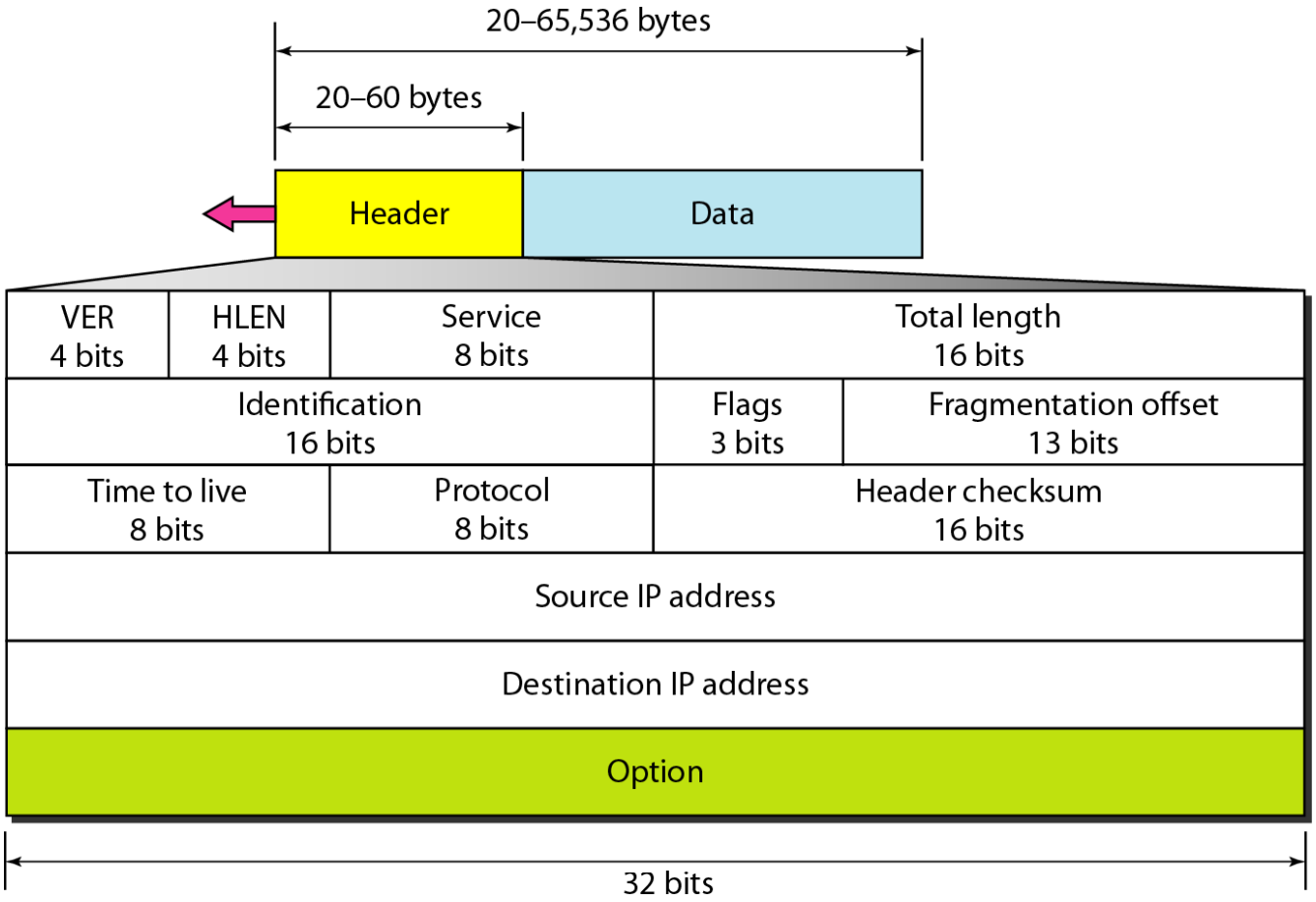
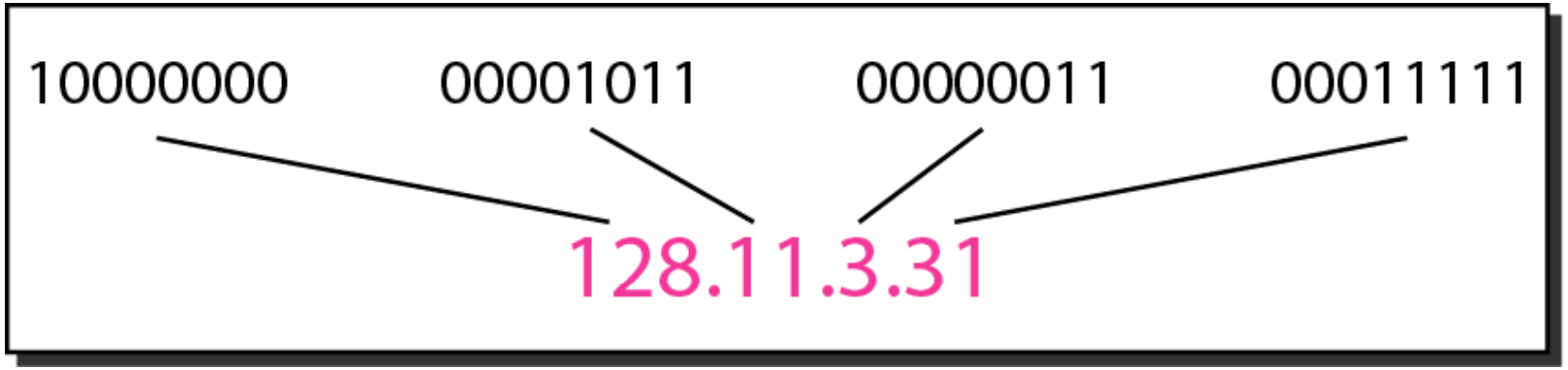


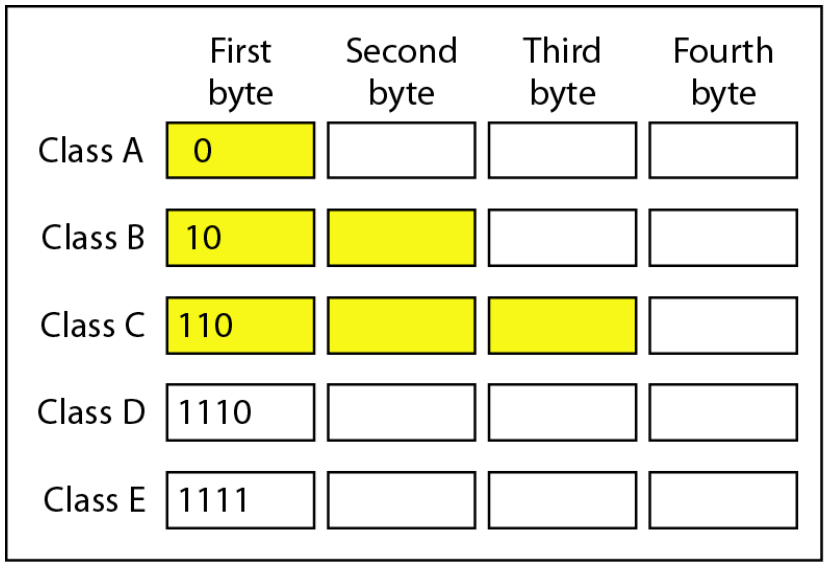
Figure 19.1 *Dotted-decimal notation and binary notation for an IPv4 address*



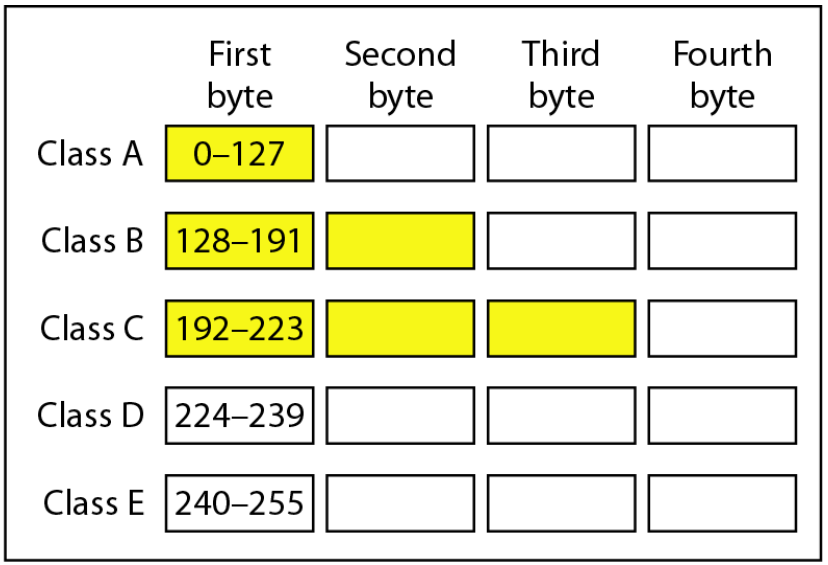
Finding the network id and the host id

- Classful
  - Classes A – E
- Classless
  - Net mask
  - (Subnetting / subnet mask)

Figure 19.2 *Finding the classes in binary and dotted-decimal notation*



a. Binary notation

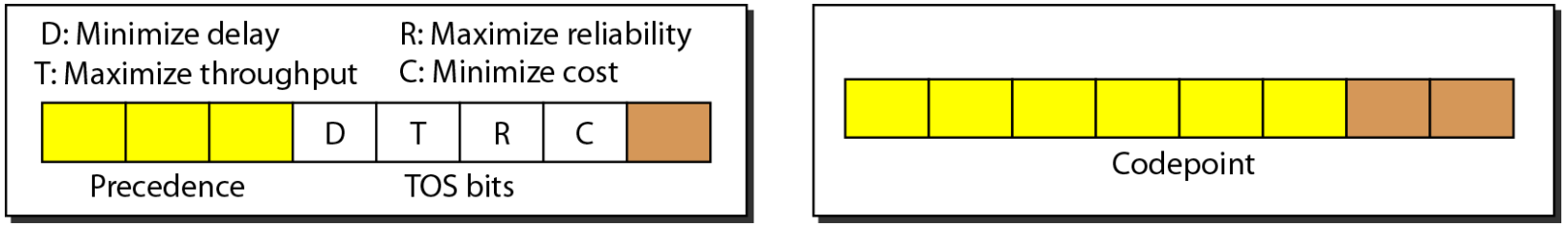


b. Dotted-decimal notation

Table 19.2 *Default masks for classful addressing*

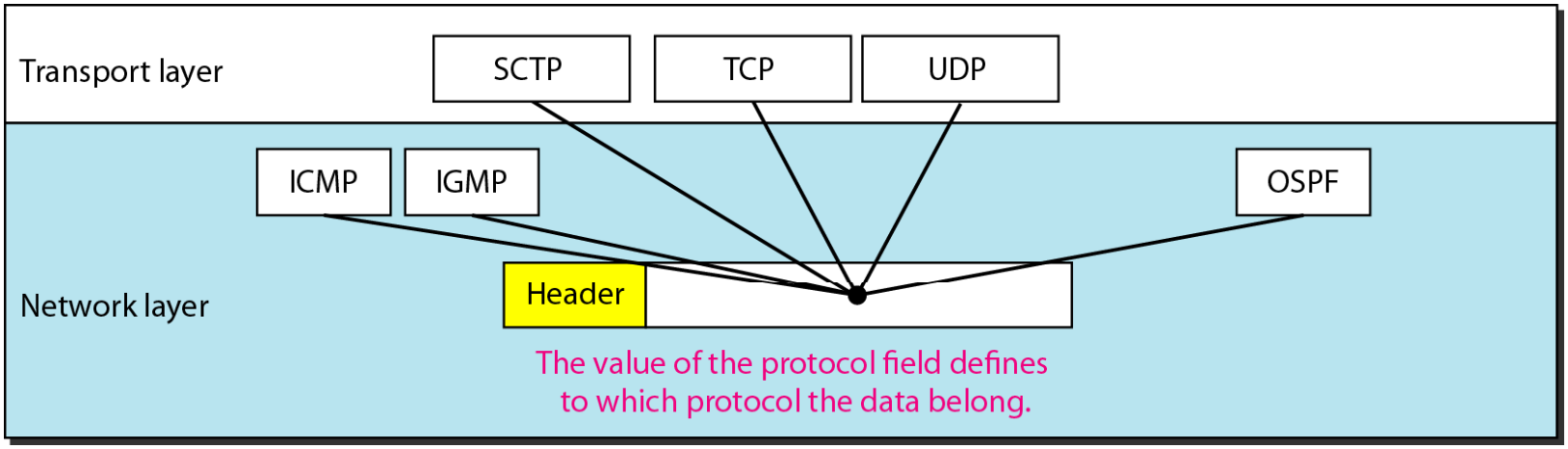
Class	*Binary*	*Dotted-Decimal*	*CIDR*
A	**11111111** 00000000 00000000 00000000	**255**.0.0.0	/8
B	**11111111 11111111** 00000000 00000000	**255.255**.0.0	/16
C	**11111111 11111111 11111111** 00000000	**255.255.255**.0	/24

Figure 20.6 *Service type or differentiated services*



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

Figure 20.8 *Protocol field and encapsulated data*



Value	*Protocol*
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

Figure 20.13 *Example of checksum calculation in IPv4*

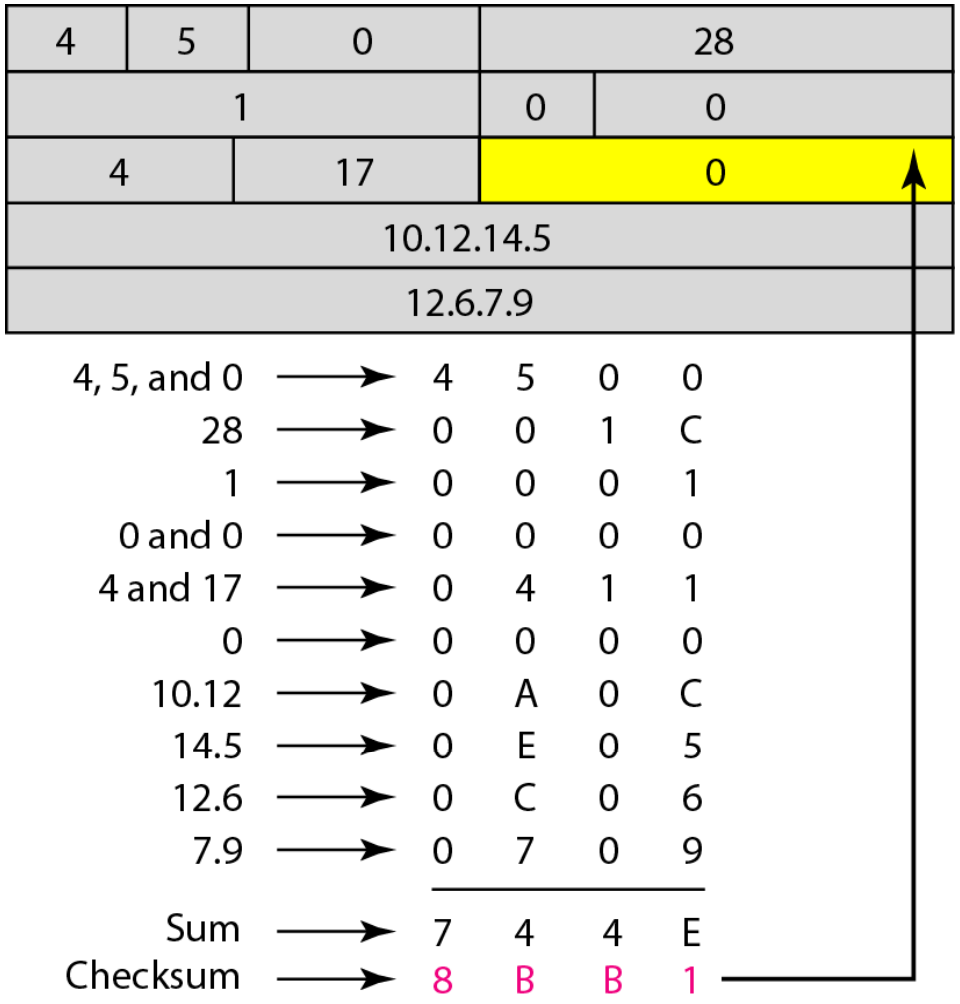


Figure 20.14 *Taxonomy of options in IPv4*

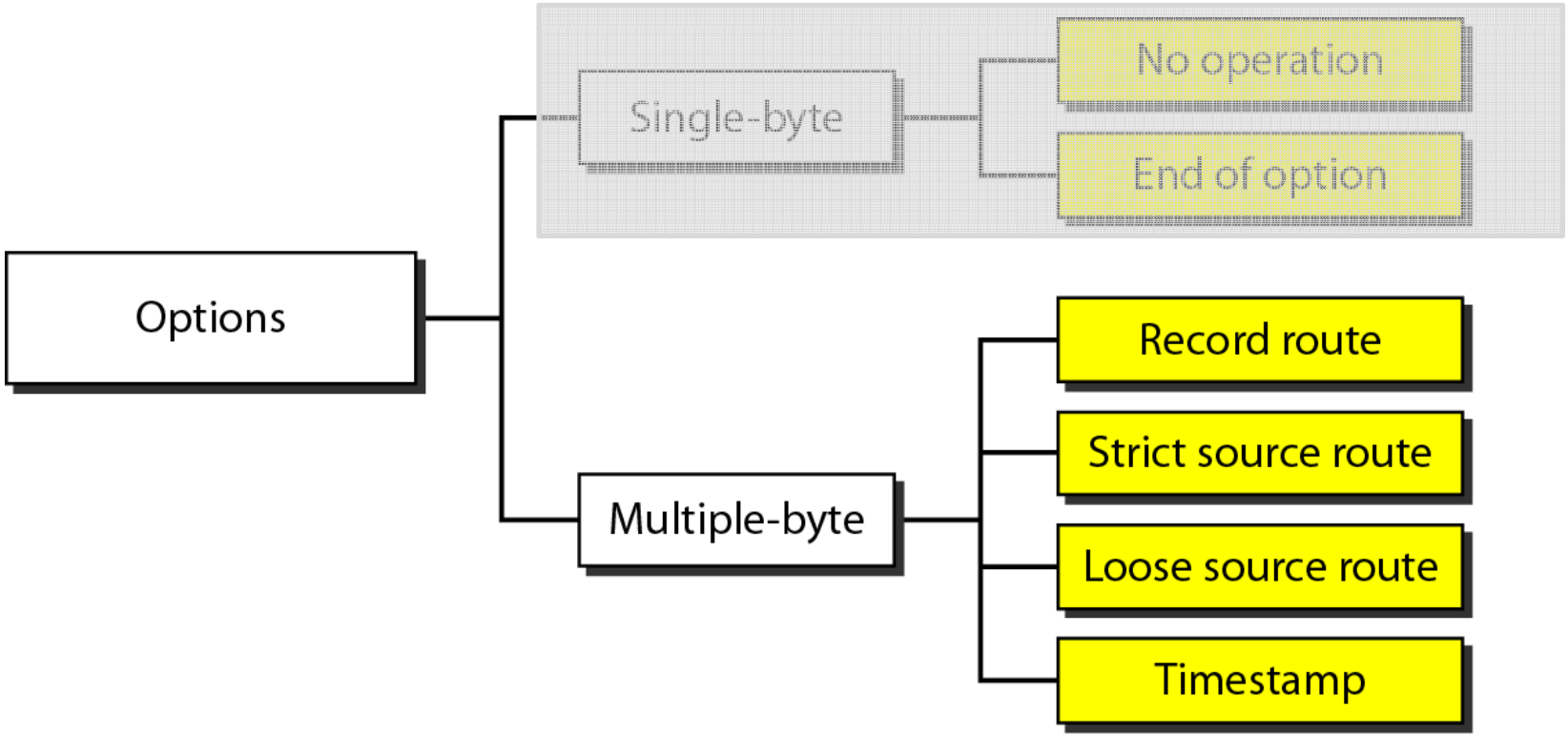
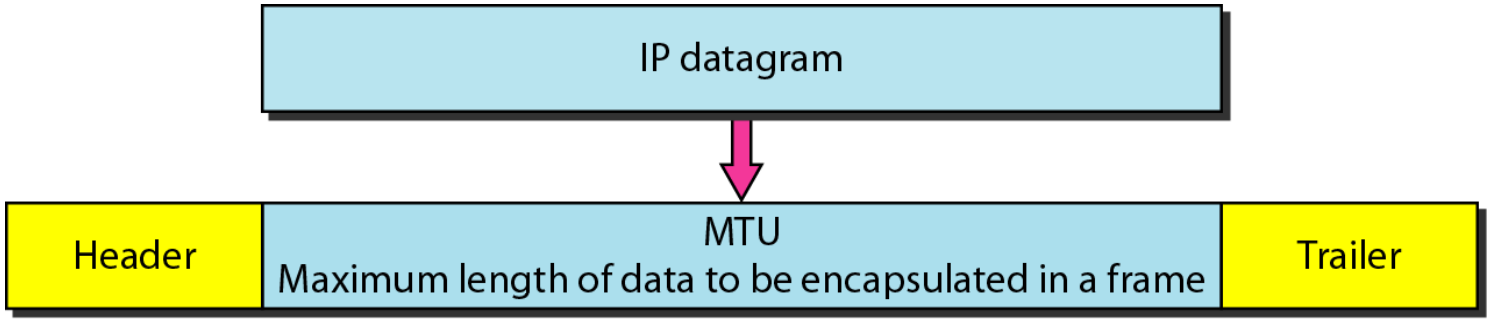


Figure 20.9 *Maximum transfer unit (MTU)*



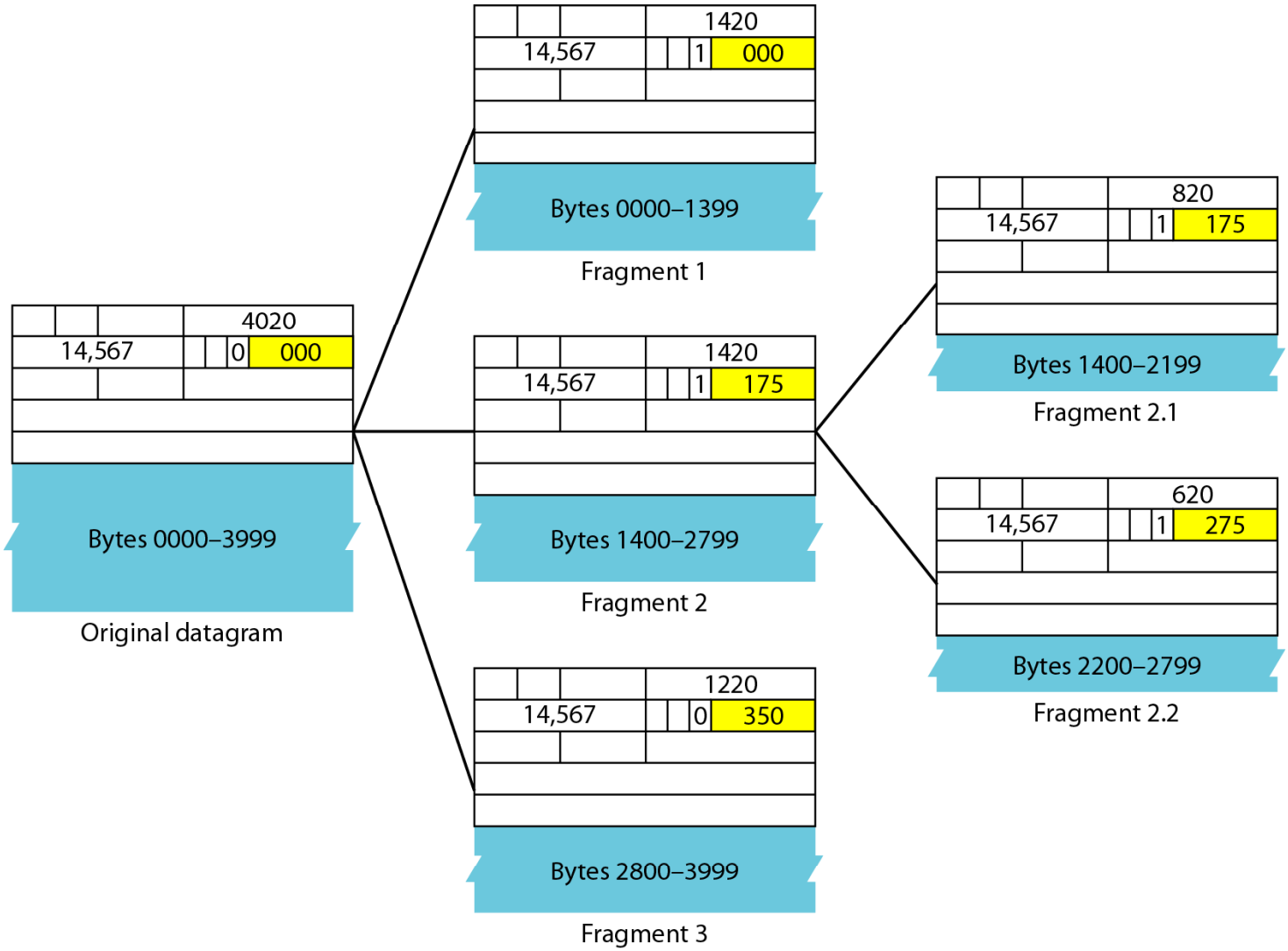
Protocol	*MTU*
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

Fragmentation (IPv4)

- Needed if IP datagram size > MTU of next link
- Framgentation performed by the router that meets the problem
- Defragmentation performed by destination host

Figure 20.10 *Flags used in fragmentation*

Figure 20.12 *Detailed fragmentation example*



IPv6

- Header
- Addresses

Figure 20.15 *IPv6 datagram header and payload*

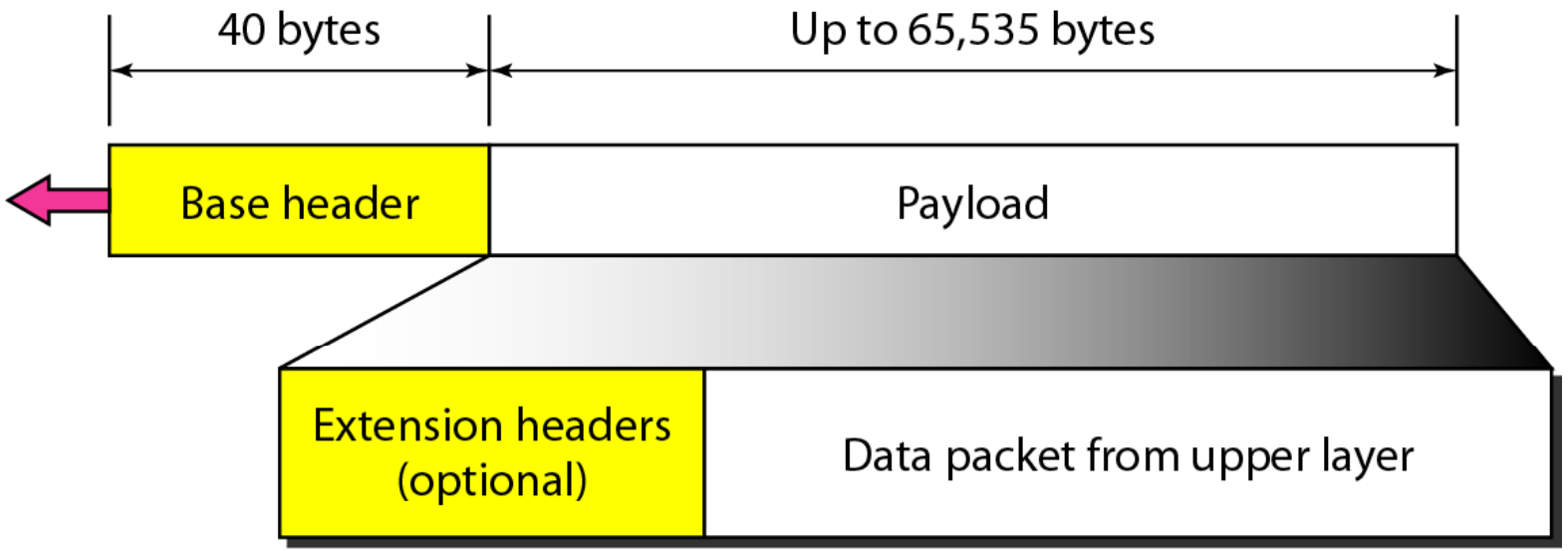


Figure 20.16 *Format of an IPv6 datagram*

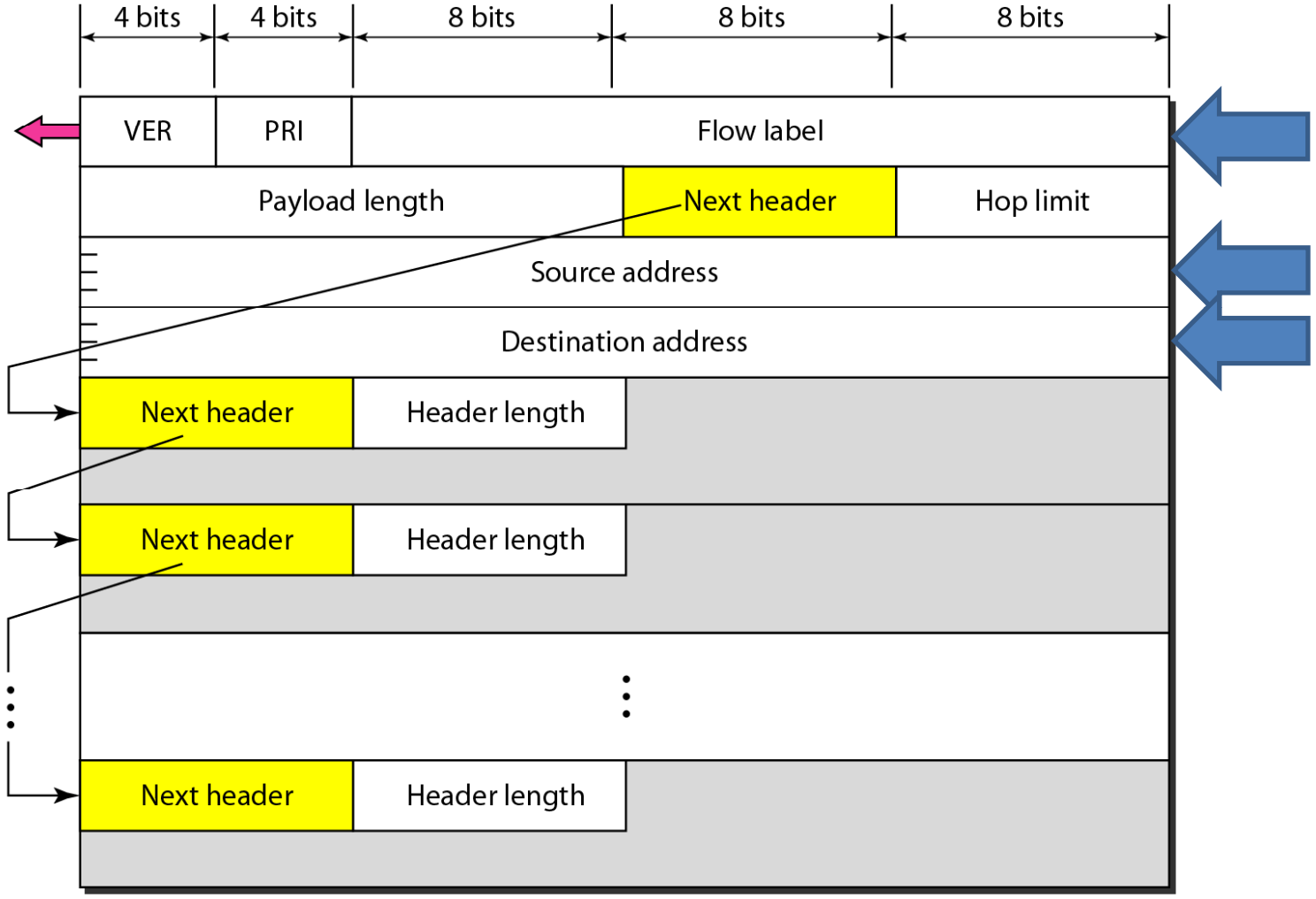
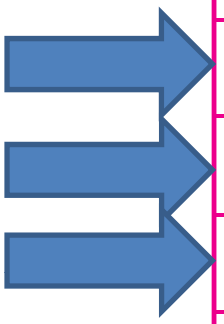


Table 20.6 *Next header codes for IPv6*



Code	*Next Header*
0	Hop-by-hop option
2	ICMP
6	TCP
17	UDP
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	Null (no next header)
60	Destination option

Figure 19.14 *IPv6 address in binary and hexadecimal colon notation*

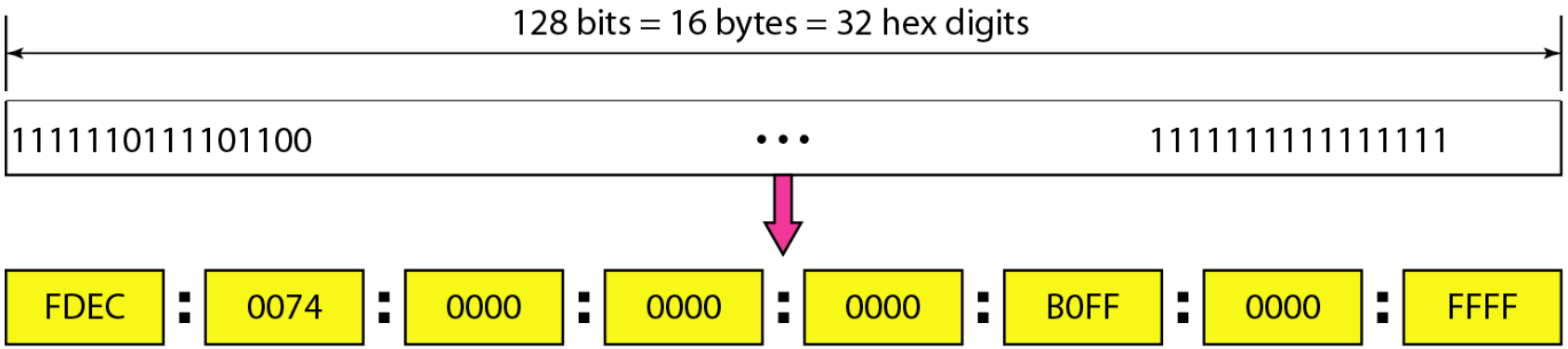


Table 20.7 *Priorities for congestion-controlled traffic*

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

Table 20.8 *Priorities for noncongestion-controlled traffic*

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

Table 20.9 *Comparison between IPv4 and IPv6 packet headers*

Comparison
1. The header length field is eliminated in IPv6 because the length of the header is fixed in this version.
2. The service type field is eliminated in IPv6. The priority and flow label fields together take over the function of the service type field.
3. The total length field is eliminated in IPv6 and replaced by the payload length field.
4. The identification, flag, and offset fields are eliminated from the base header in IPv6. They are included in the fragmentation extension header.
5. The TTL field is called hop limit in IPv6.
6. The protocol field is replaced by the next header field.
7. The header checksum is eliminated because the checksum is provided by upper-layer protocols; it is therefore not needed at this level.
8. The option fields in IPv4 are implemented as extension headers in IPv6.

Figure 20.17 *Extension header types*

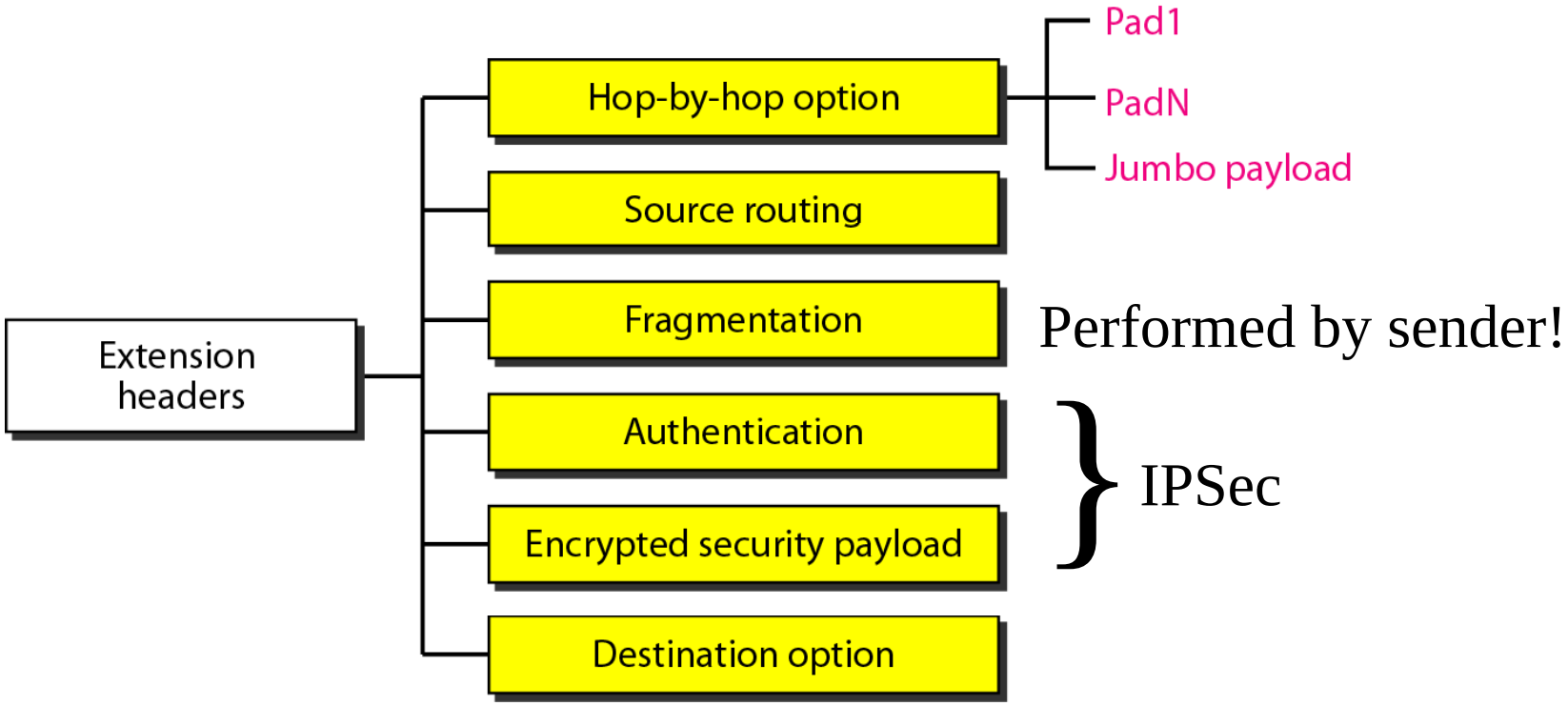


Table 20.10 *Comparison between IPv4 options and IPv6 extension headers*

Comparison
1. The no-operation and end-of-option options in IPv4 are replaced by Pad1 and PadN options in IPv6.
2. The record route option is not implemented in IPv6 because it was not used.
3. The timestamp option is not implemented because it was not used.
4. The source route option is called the source route extension header in IPv6.
5. The fragmentation fields in the base header section of IPv4 have moved to the fragmentation extension header in IPv6.
6. The authentication extension header is new in IPv6.
7. The encrypted security payload extension header is new in IPv6.

Transition IPv4 -> IPv6

- Cannot be made at one occasion
  - Both protocols must coexist
    - Networks nodes
    - Hosts (remember not only computers are hosts)
- Economic costs versus actual need
  - IPv4 address space lasts longer than expected
    - CIDR (Classless Inter Domain Routing)
    - NAT (Network Address Translation)

Figure 20.18 *Three transition strategies*

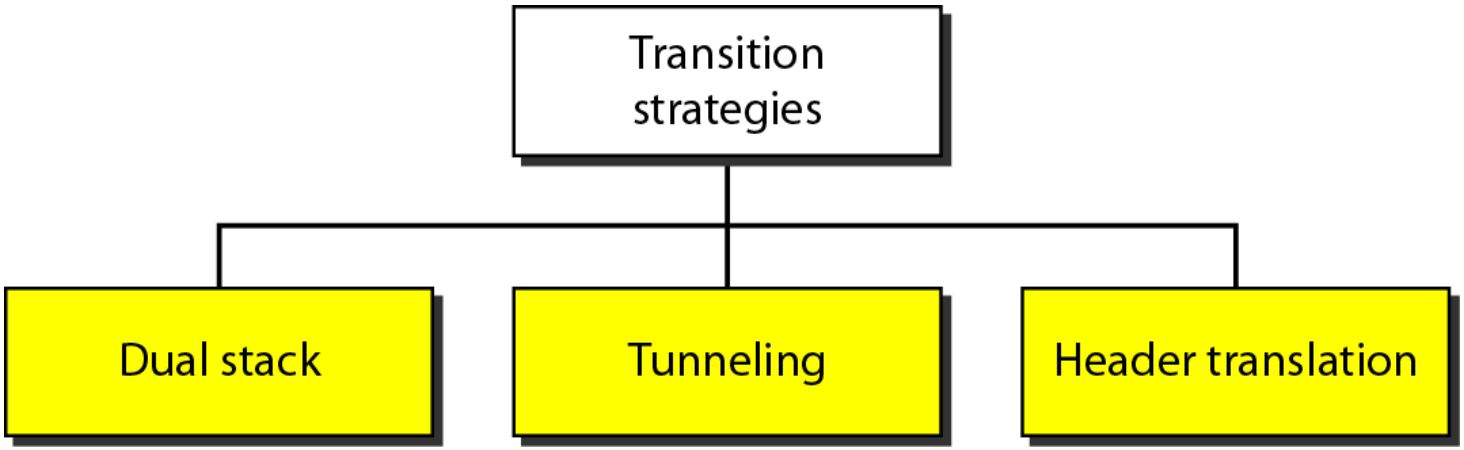


Figure 20.19 *Dual stack*

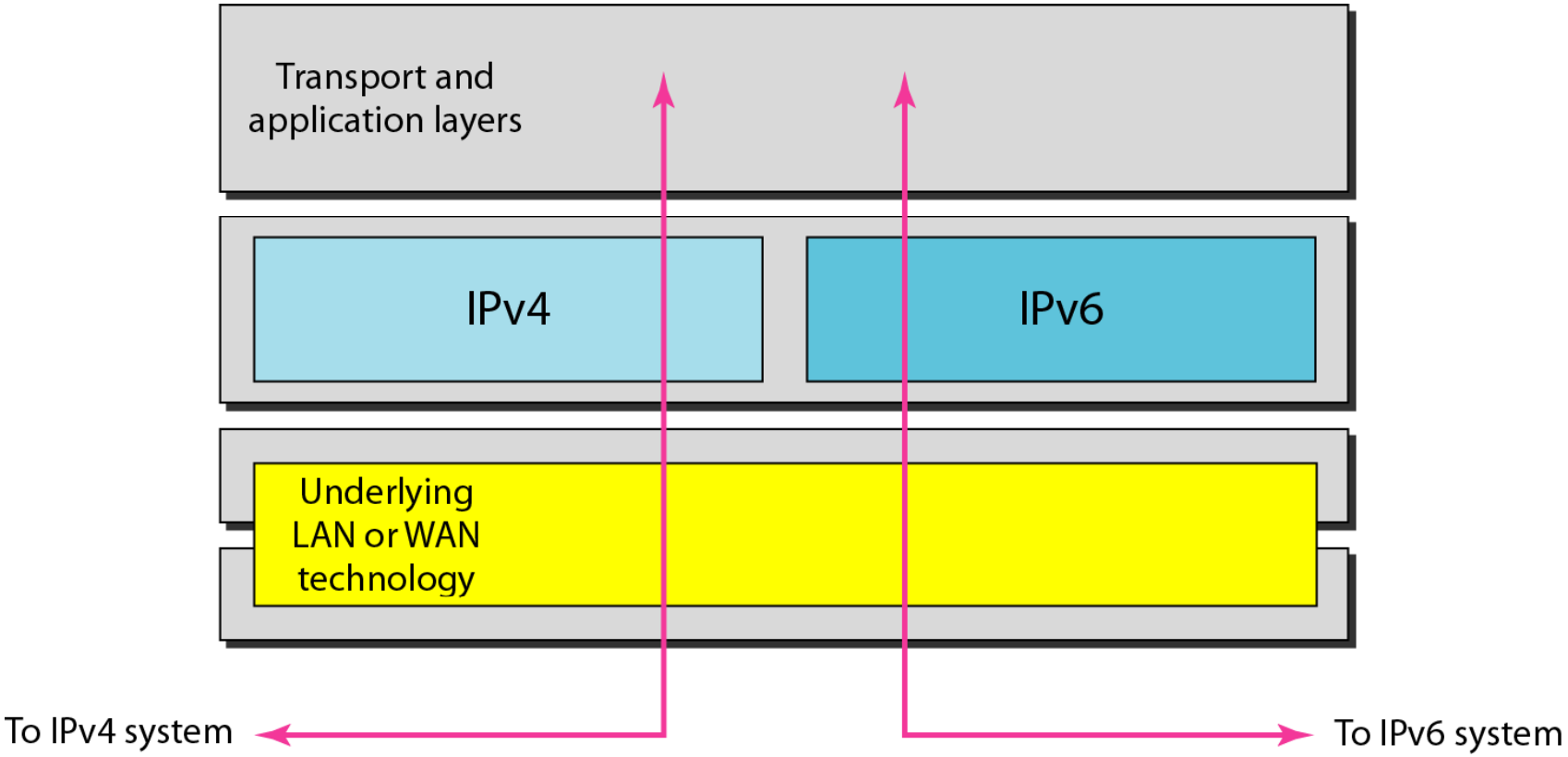


Figure 20.20 *Tunneling strategy*

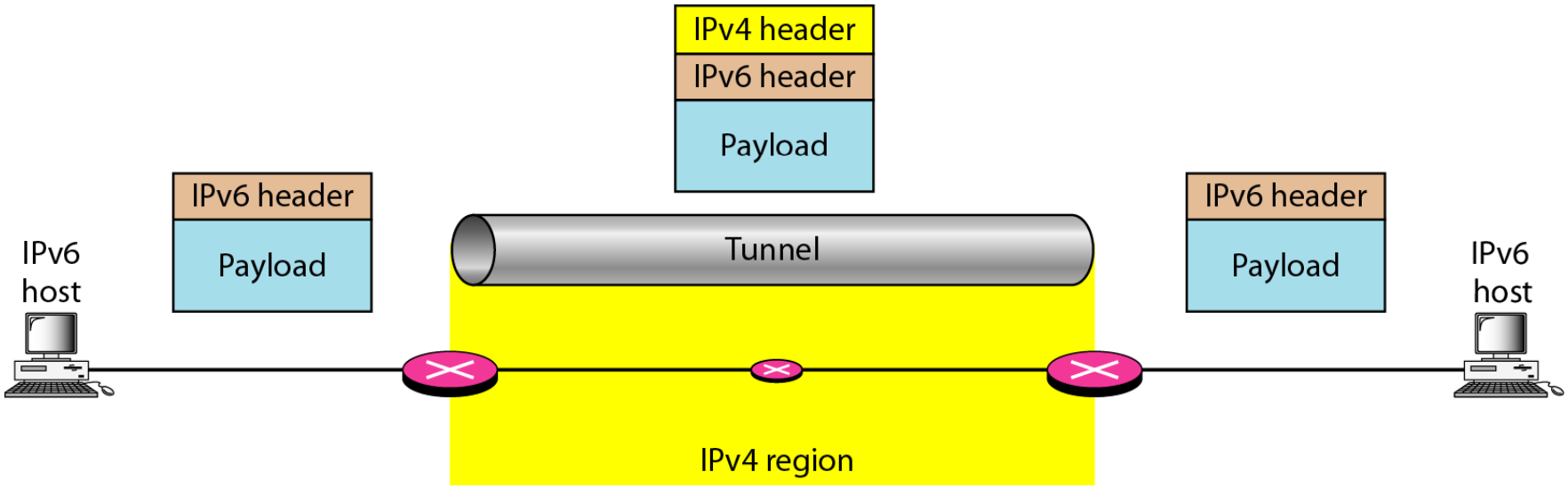


Figure 20.21 *Header translation strategy*

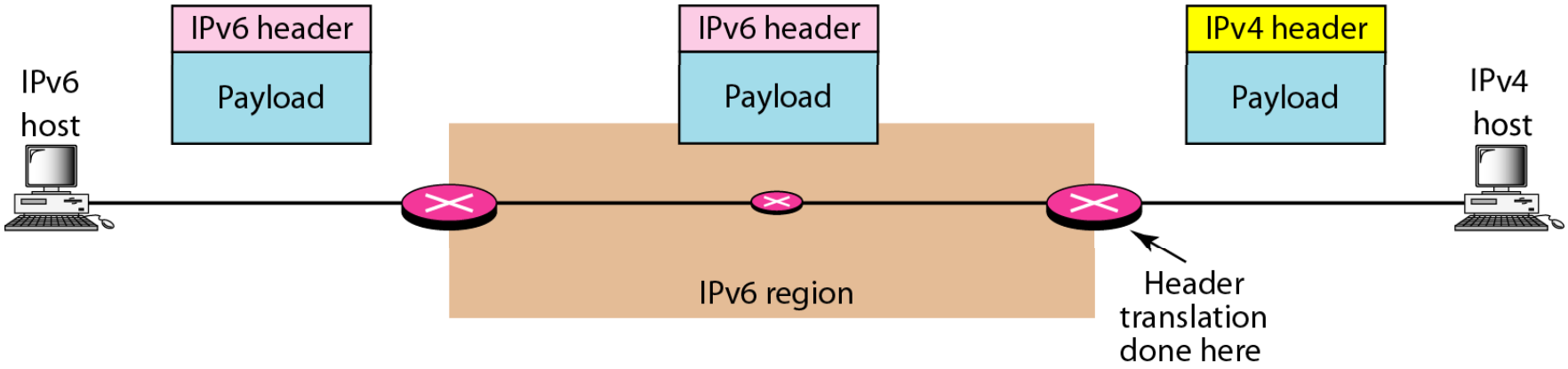


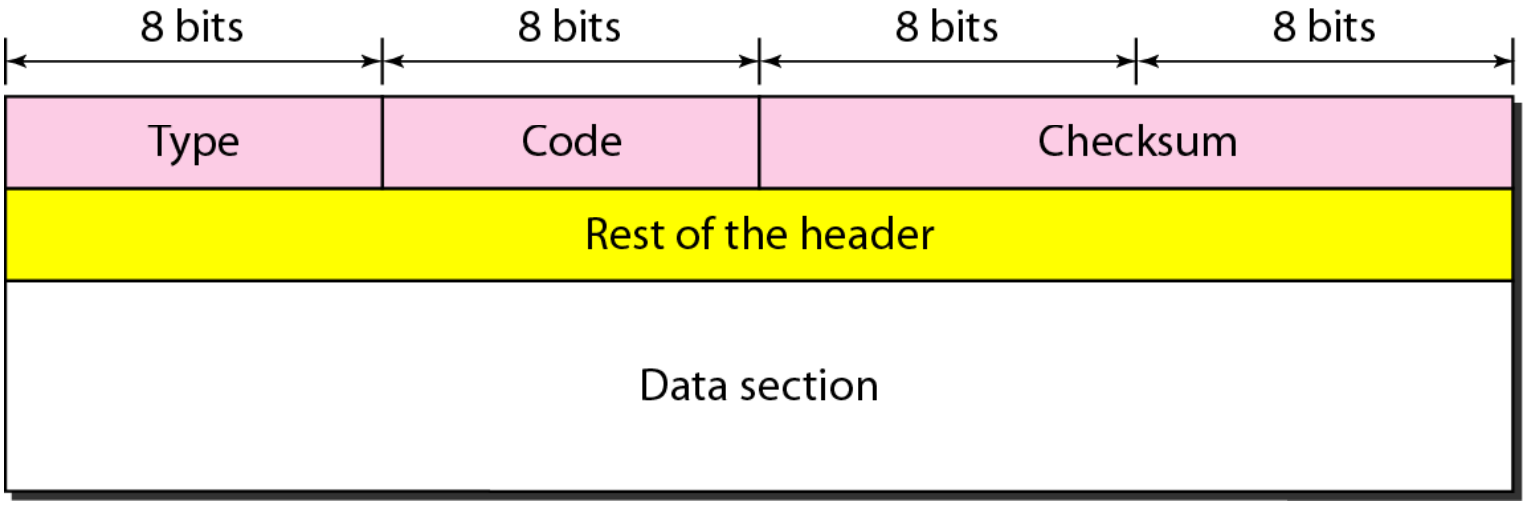
Table 20.11 *Header translation*

Header Translation Procedure
1. The IPv6 mapped address is changed to an IPv4 address by extracting the rightmost 32 bits.
2. The value of the IPv6 priority field is discarded.
3. The type of service field in IPv4 is set to zero.
4. The checksum for IPv4 is calculated and inserted in the corresponding field.
5. The IPv6 flow label is ignored.
6. Compatible extension headers are converted to options and inserted in the IPv4 header. Some may have to be dropped.
7. The length of IPv4 header is calculated and inserted into the corresponding field.
8. The total length of the IPv4 packet is calculated and inserted in the corresponding field.

ICMP

- Internet Control Message Protocol
- Supplementory support protocol for IP
  - Error-reporting
  - Queries

Figure 21.8 *General format of ICMP messages*



Notes on ICMP

- No ICMP error message will be generated in response to a datagram carrying an ICMP error message.
- No ICMP error message will be generated for a fragmented datagram that is not the first fragment.
- No ICMP error message will be generated for a datagram having a multicast address.
- No ICMP error message will be generated for a datagram having a special address such as 127.0.0.0 or 0.0.0.0.

Figure 21.9 *Error-reporting messages*

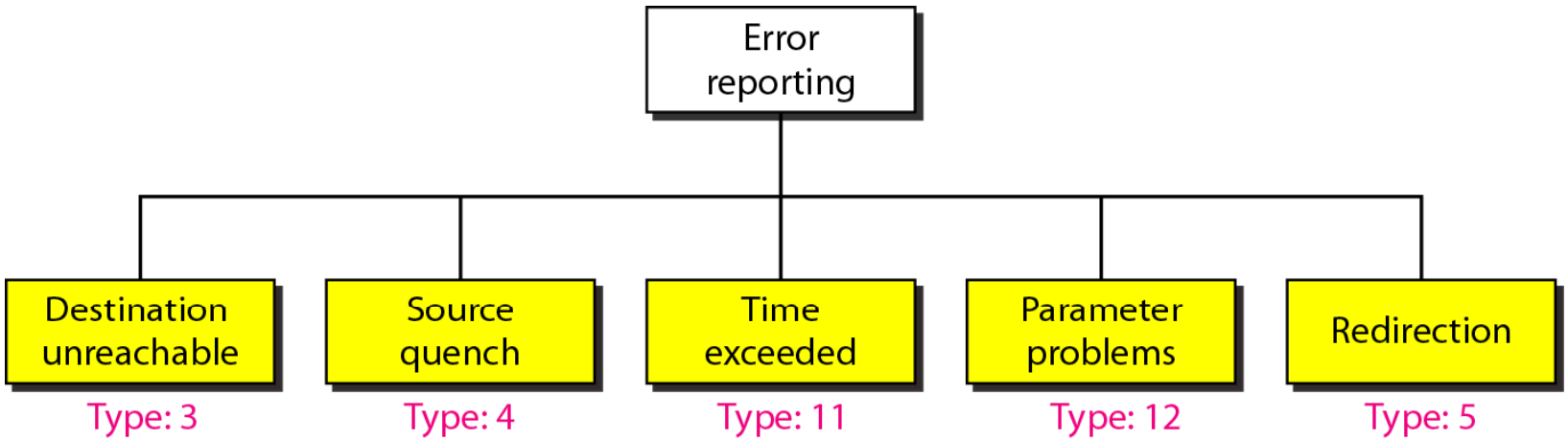


Figure 21.10 *Contents of data field for the error messages*

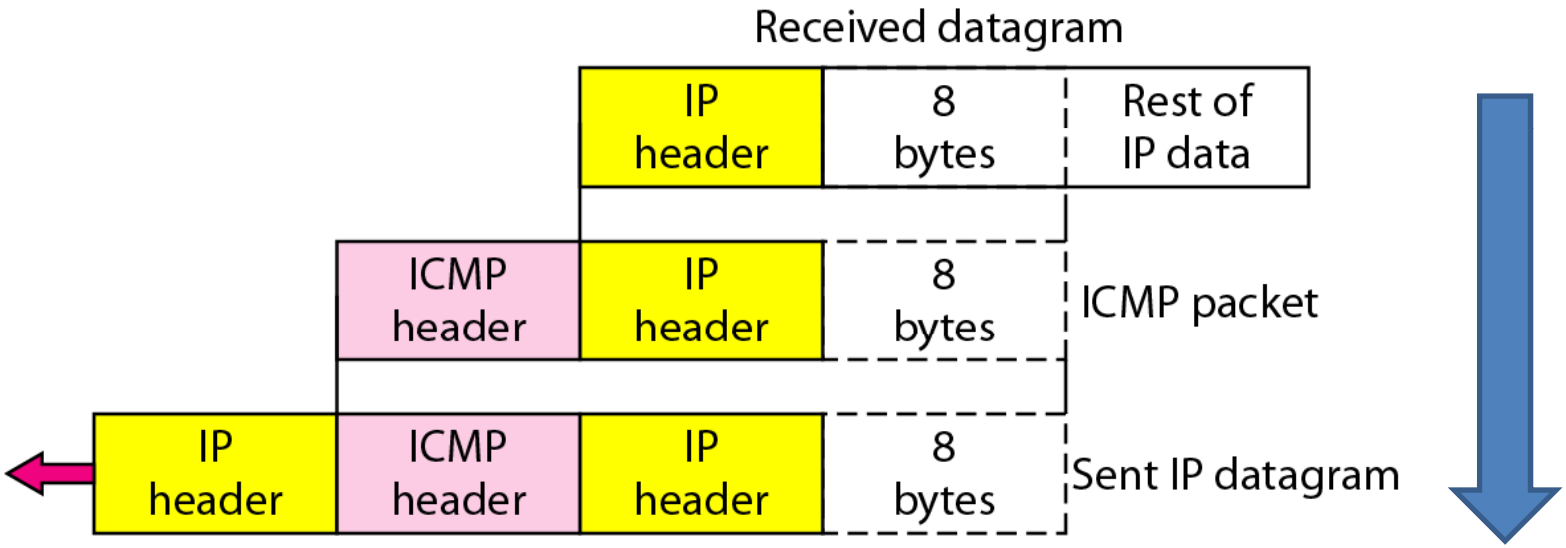


Figure 21.11 *Redirection concept*

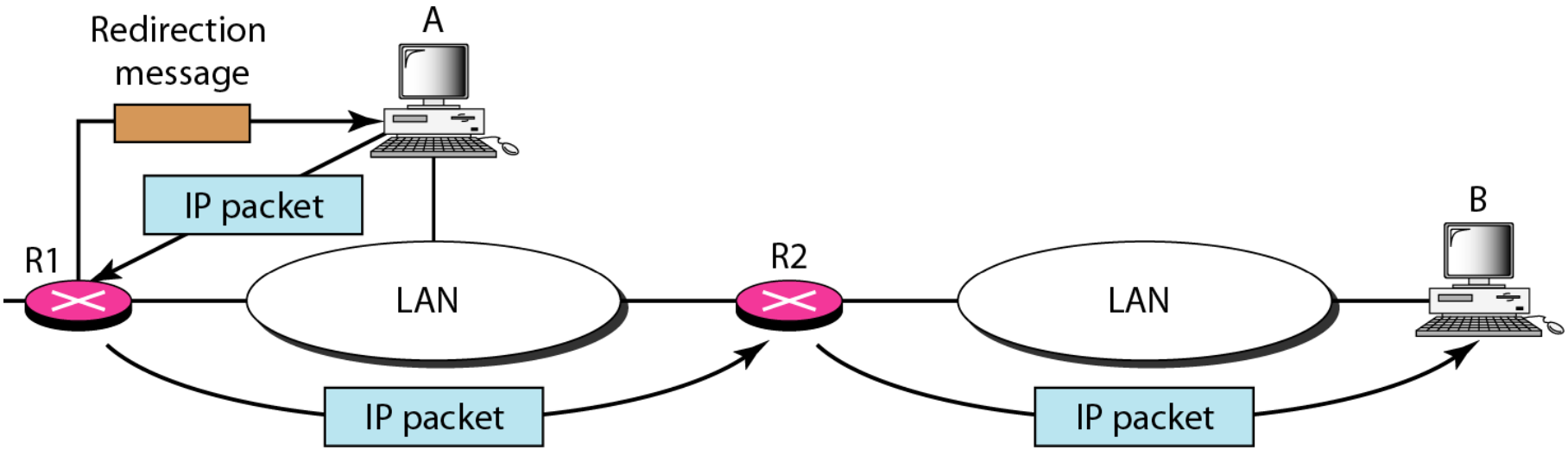


Figure 21.12 *Query messages*

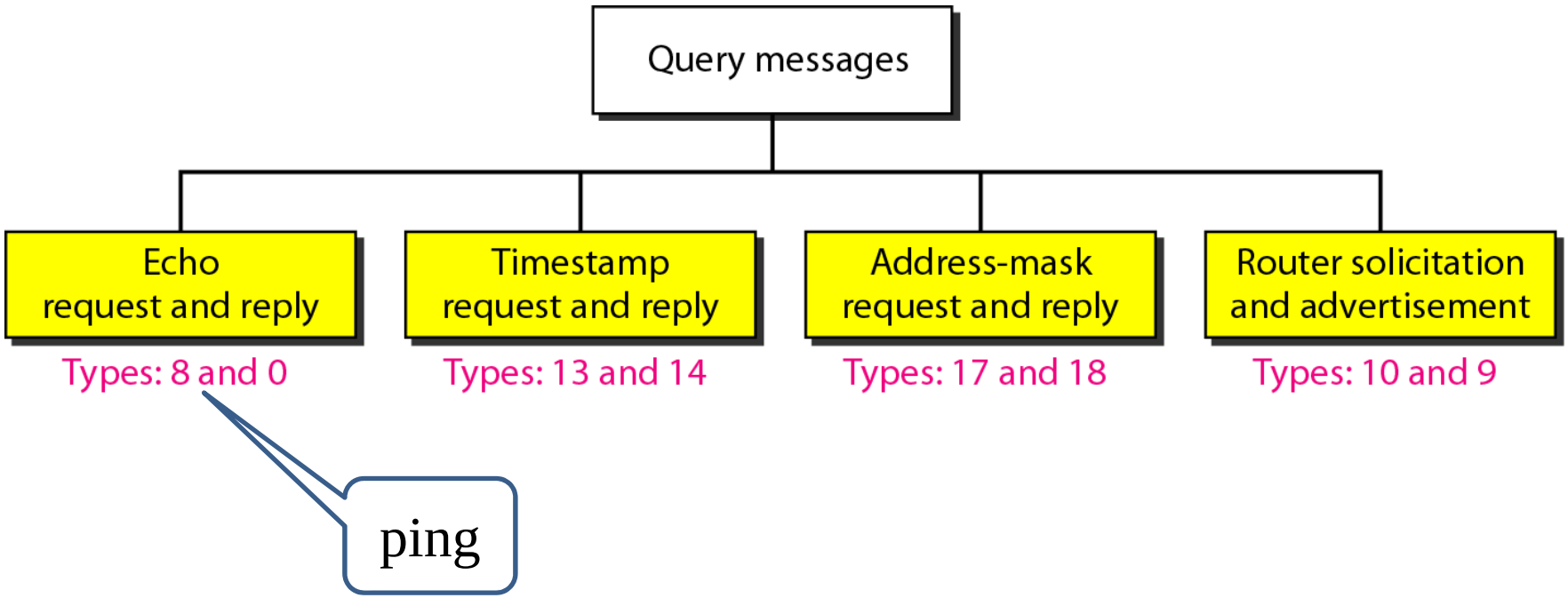


Figure 21.13 *Encapsulation of ICMP query messages*

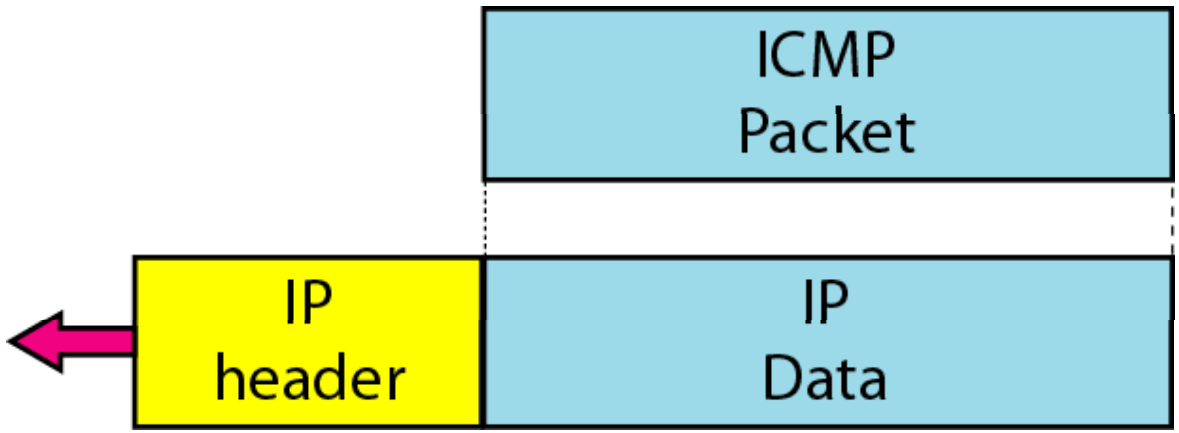


Figure 21.23 *Comparison of network layers in version 4 and version 6*

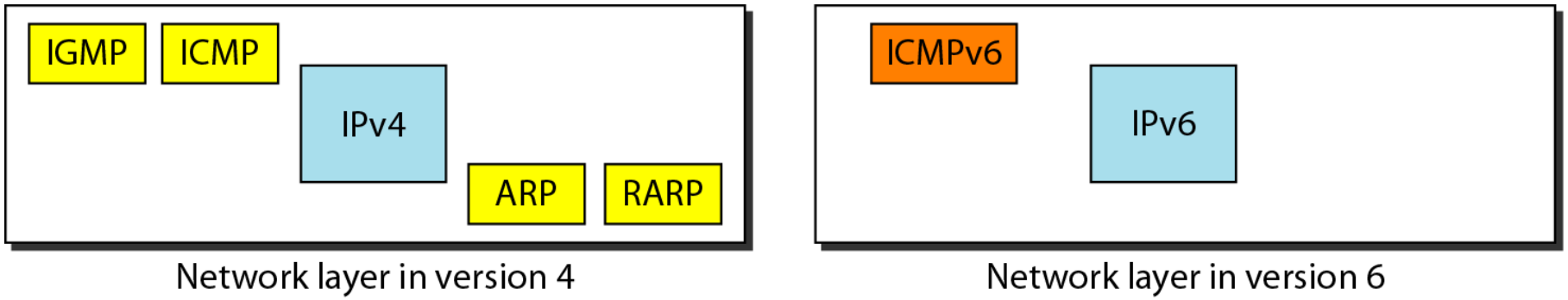


Table 21.3 *Comparison of error-reporting messages in ICMPv4 and ICMPv6*

Type of Message	*Version 4*	*Version 6*
Destination unreachable	Yes	Yes
Source quench	Yes	No
Packet too big	No	Yes
Time exceeded	Yes	Yes
Parameter problem	Yes	Yes
Redirection	Yes	Yes

Table 21.4 *Comparison of query messages in ICMPv4 and ICMPv6*

Type of Message	*Version 4*	*Version 6*
Echo request and reply	Yes	Yes
Timestamp request and reply	Yes	No
Address-mask request and reply	Yes	No
Router solicitation and advertisement	Yes	Yes
Neighbor solicitation and advertisement	ARP	Yes
Group membership	IGMP	Yes

RTP, RTCP

- Real Time Protocol
- Real Time Control Protocol
- No delivery mechanism
  - Uses UDP/IP
- Contributions
  - Time-stampning
  - Sequencing
  - Mixing

Figure 29.18 *RTP*

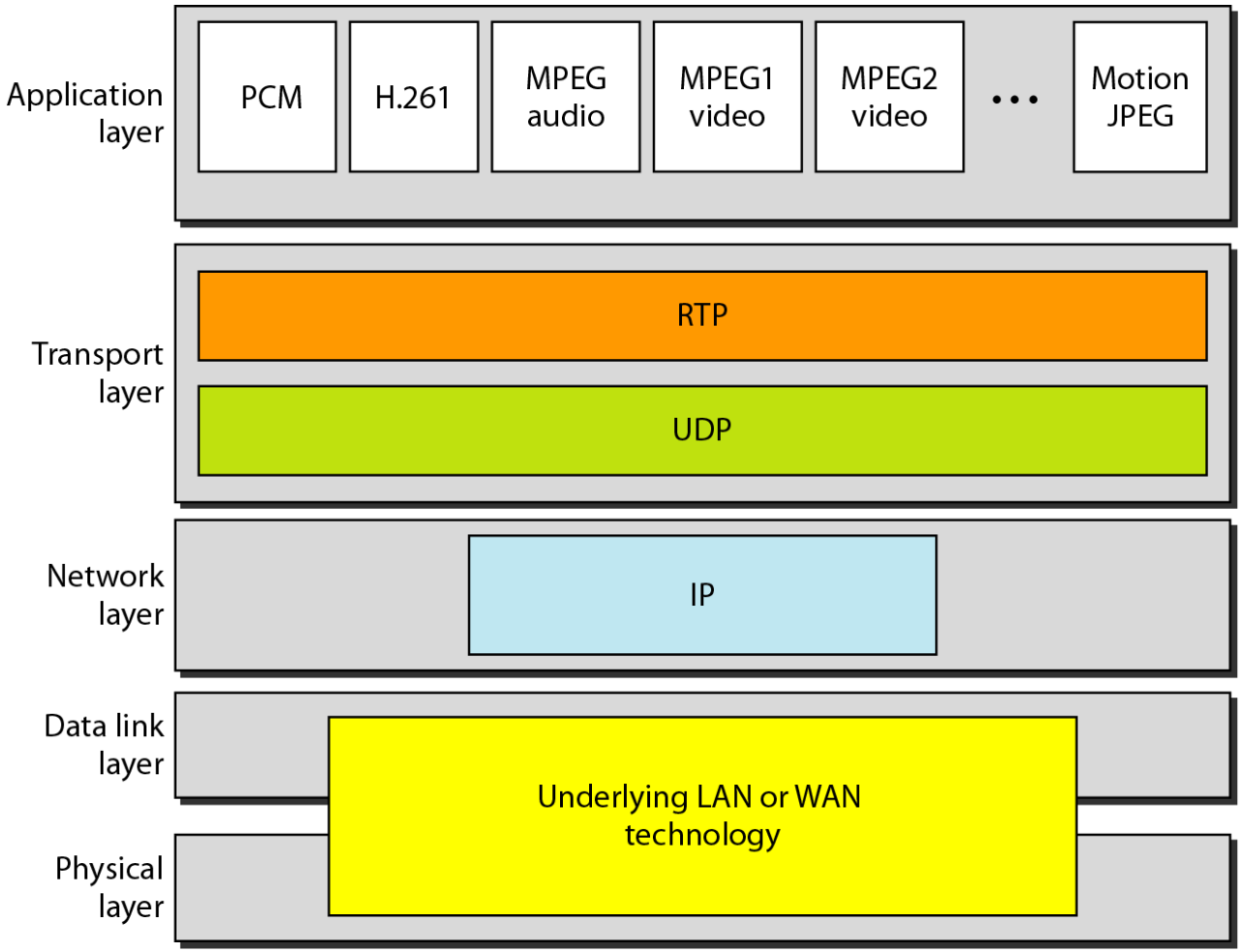


Figure 29.19 *RTP packet header format*

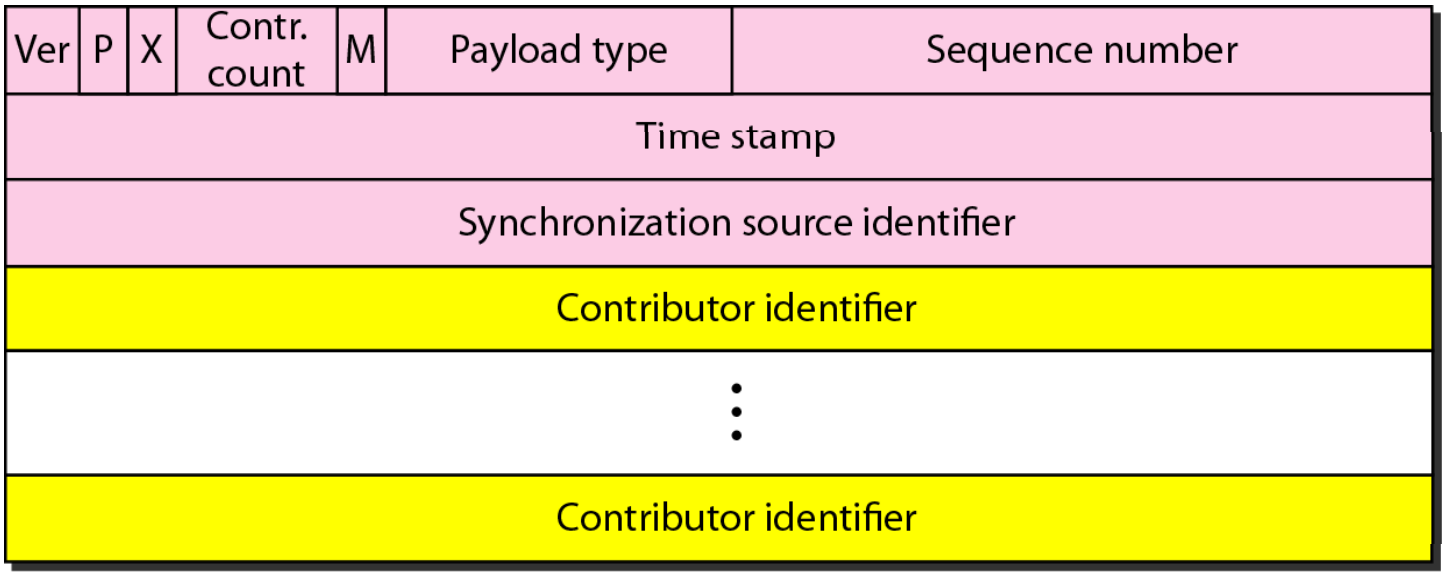


Figure 29.14 *Time relationship*

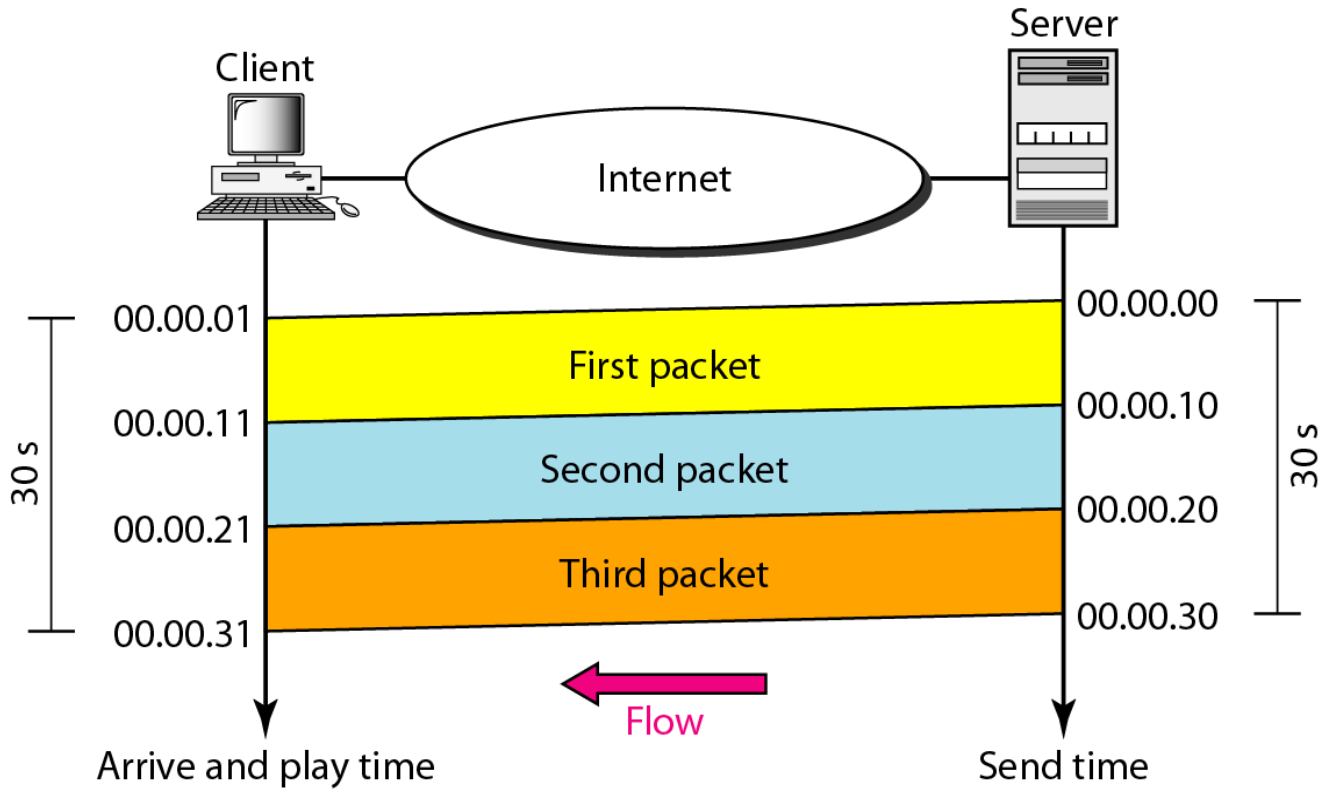


Figure 29.15 *Jitter*

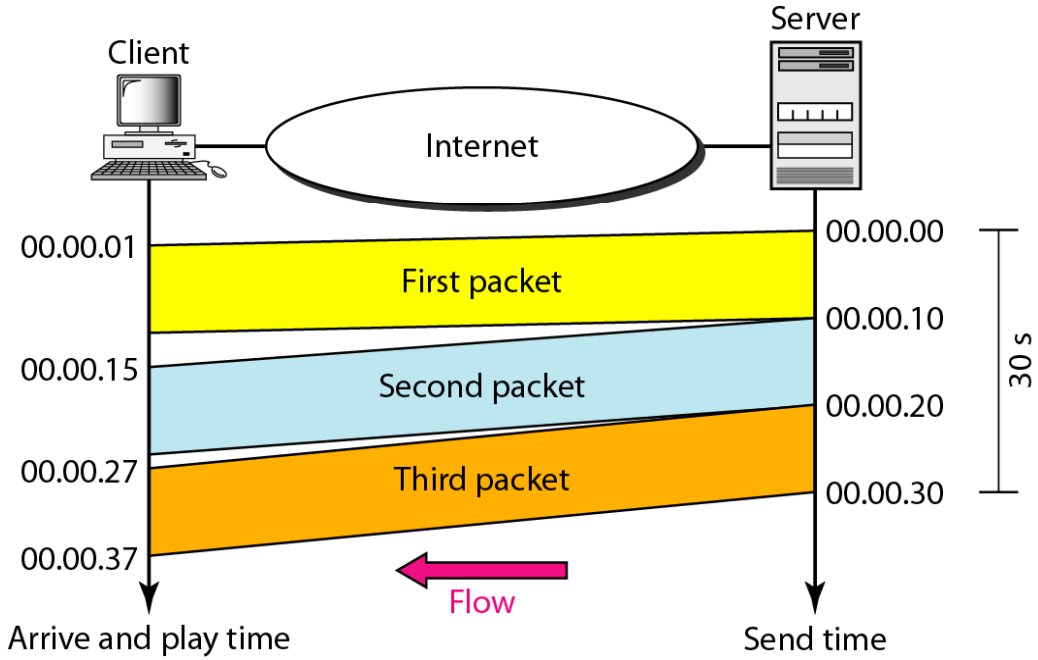


Figure 29.16 *Timestamp*

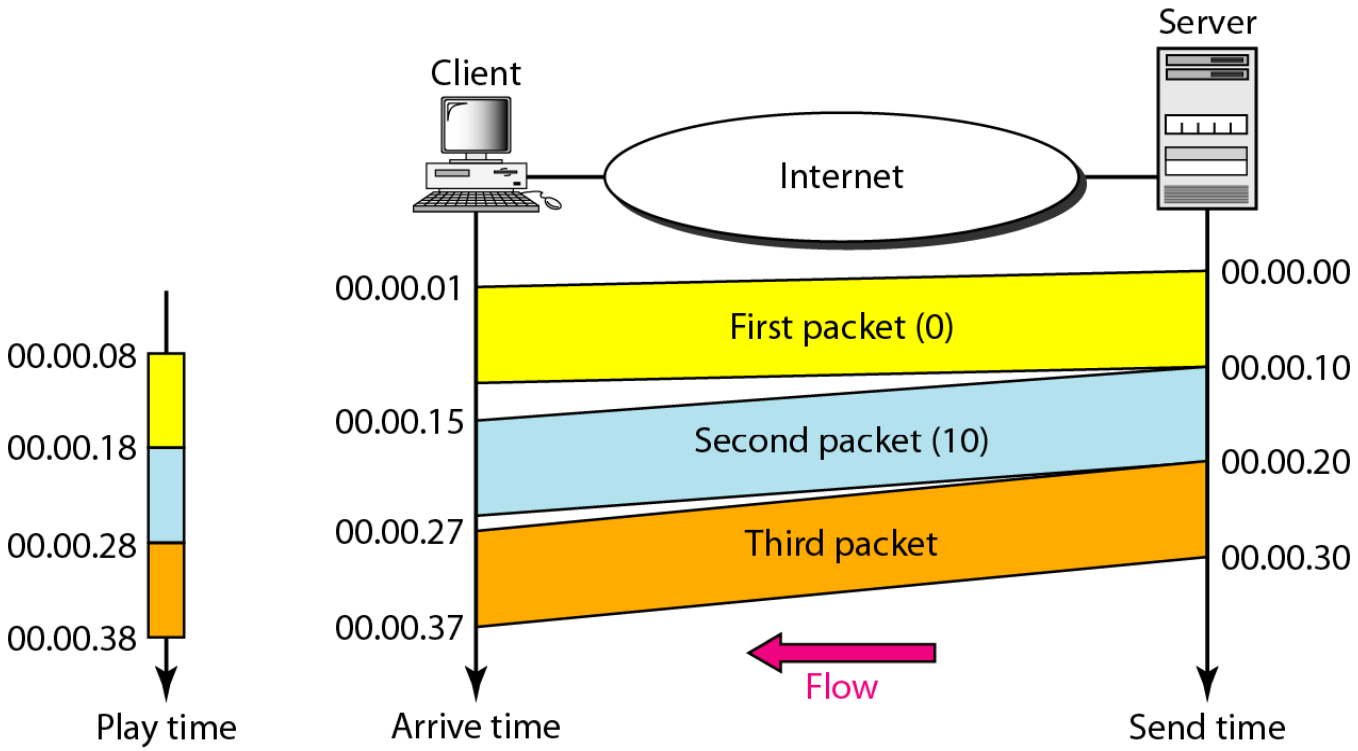
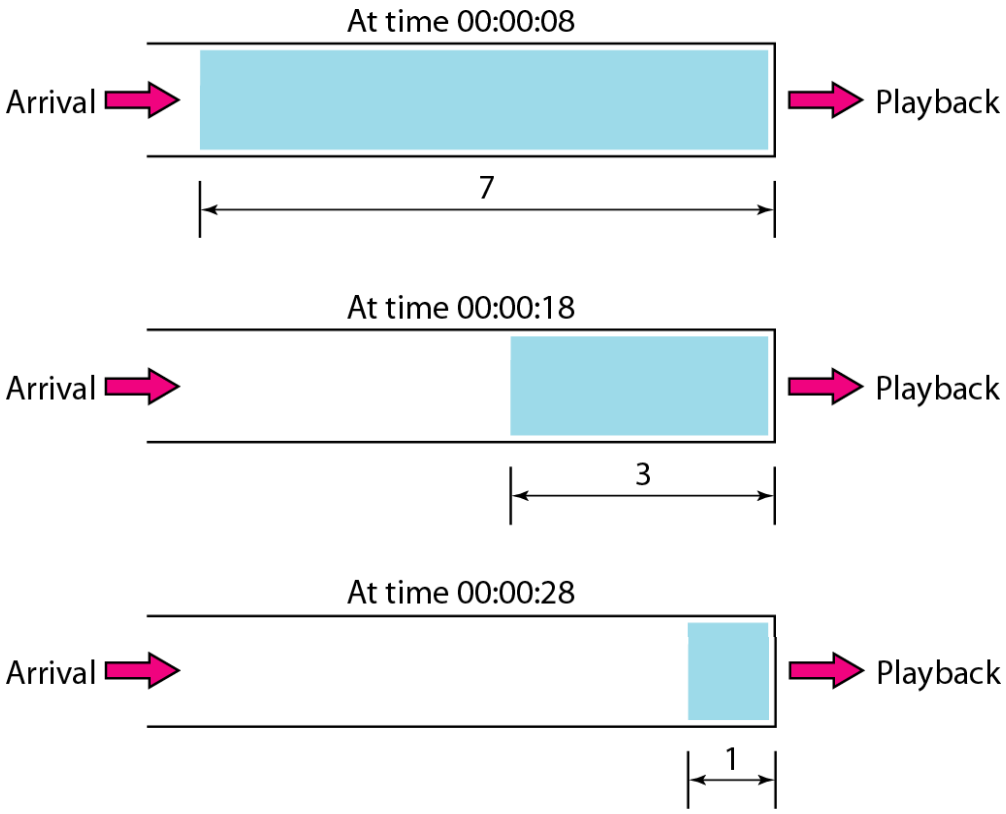


Figure 29.17 *Playback buffer*



Sequence numbers

- Packets can be delivered out of order
- We must order the packets in the playback buffer.
- Playout according to time stamps ”fixes” lost packets.

Table 20.1 *Payload types*

Type	*Application*	*Type*	*Application*	*Type*	*Application*
0	PCMμ Audio	7	LPC audio	15	G728 audio
1	1016	8	PCMA audio	26	Motion JPEG
2	G721 audio	9	G722 audio	31	H.261
3	GSM audio	10–11	L16 audio	32	MPEG1 video
5–6	DV14 audio	14	MPEG audio	33	MPEG2 video

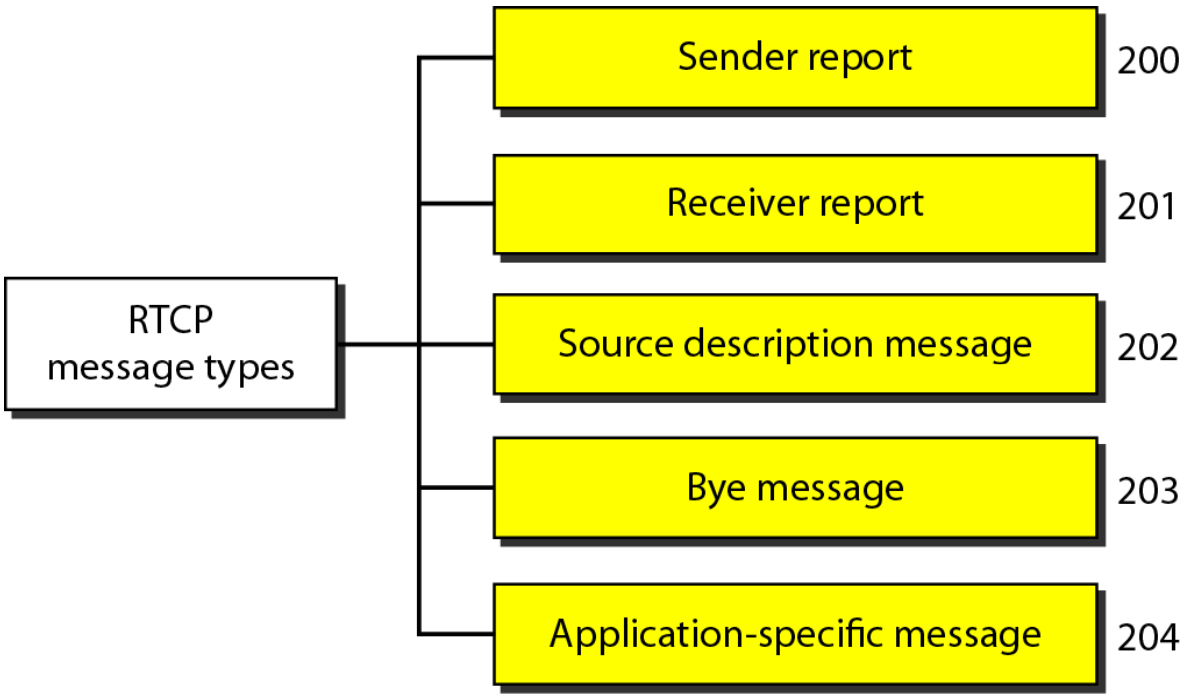
Note

RTP uses a temporary even-numbered UDP port.

RTCP

- RTP only carries data
- RTCP
  - Control messages:
    - Flow control
    - Service quality
    - Feedback to source

Figure 29.20 *RTCP message types*



Sender report

- Sent periodically by active senders
- Statistics
  - Transmission
  - Reception
- Absolute timestamp
  - # of seconds since 1970-01-01
  - Receiver can synch RTP messages
    - Important to synch audio and video

Receiver report

- Sent by passive (non sending) listeners
- Inform senders about QoS

Note

RTCP uses an odd-numbered UDP port number that follows the port number selected for RTP.

Voice over IP (VoIP)

- Internet telephony
- SIP
  - Session Initiation Protocol
- H.323
  - ITU standard

SIP

- Establish, manage, terminate multimedia sessions
- Text-based
- Six messages defined

Figure 29.21 *SIP messages*

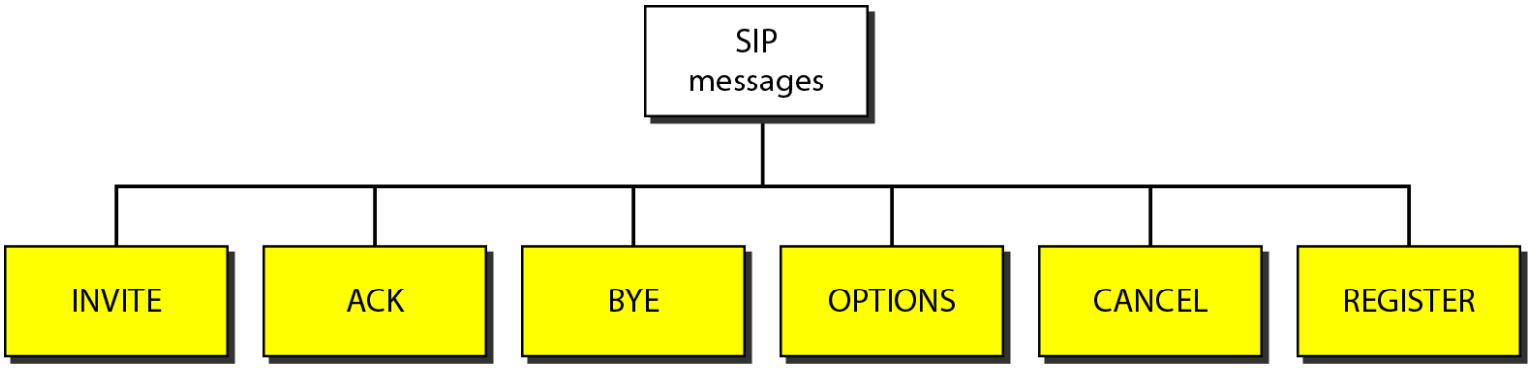


Figure 29.22 *SIP address formats*

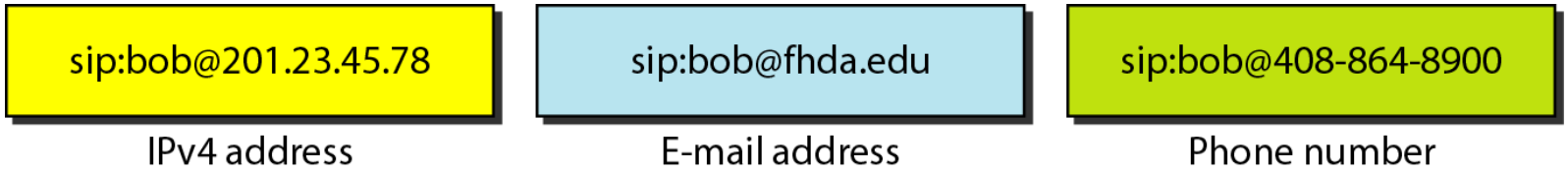


Figure 29.23 *SIP simple session*

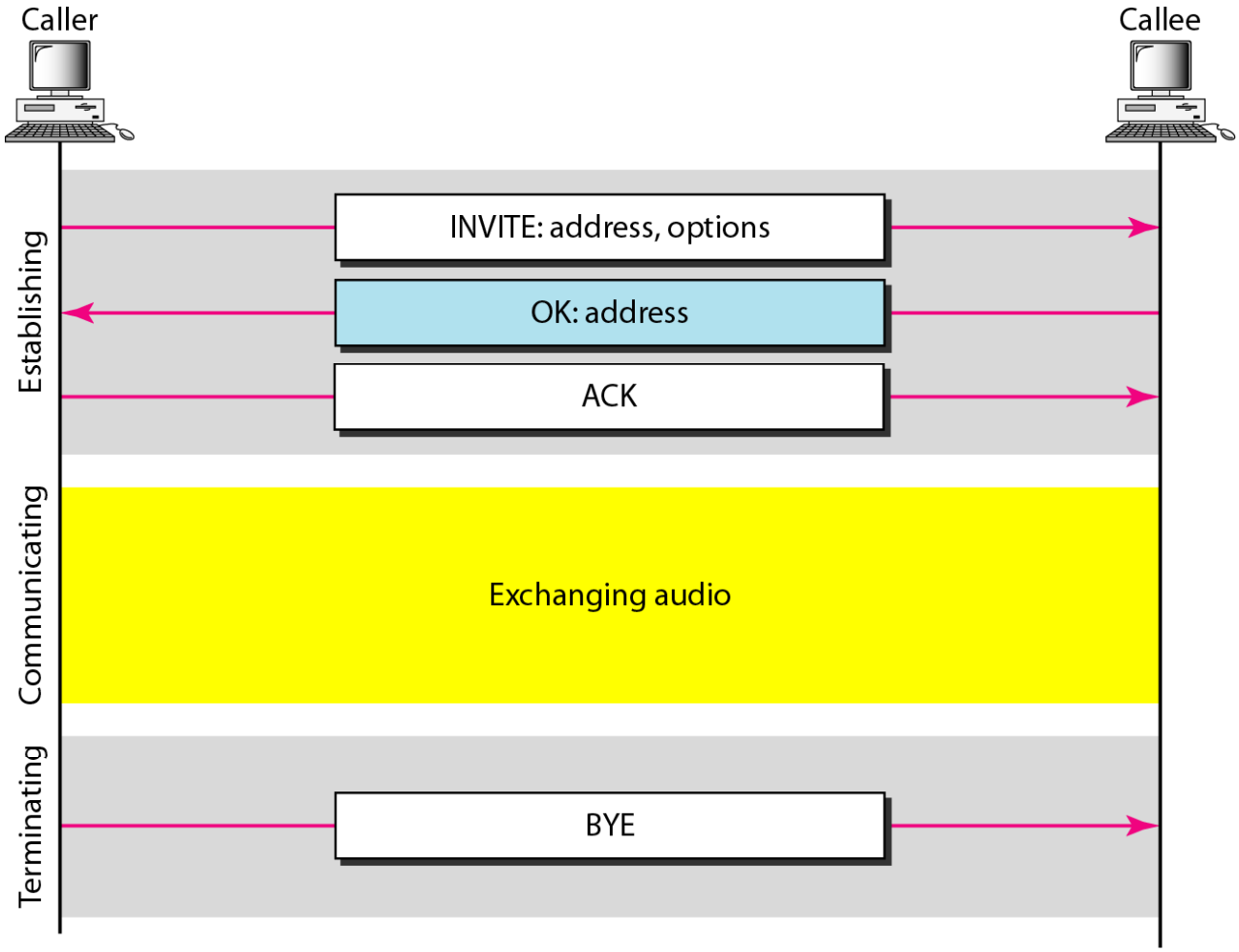
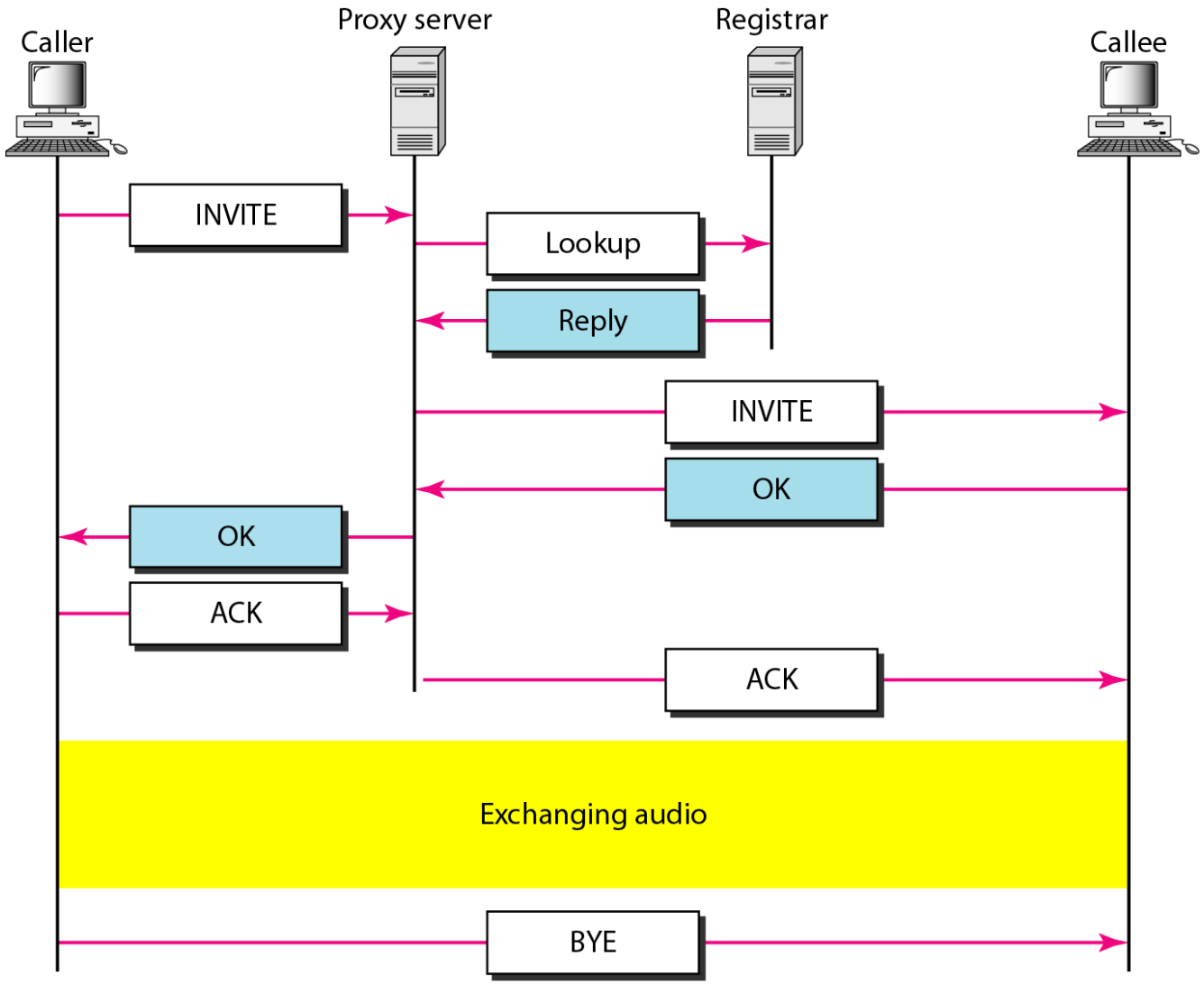


Figure 29.24 *Tracking the callee*



H.323

- Allows for communication telephone -- computer

Figure 29.25 *H.323 architecture*

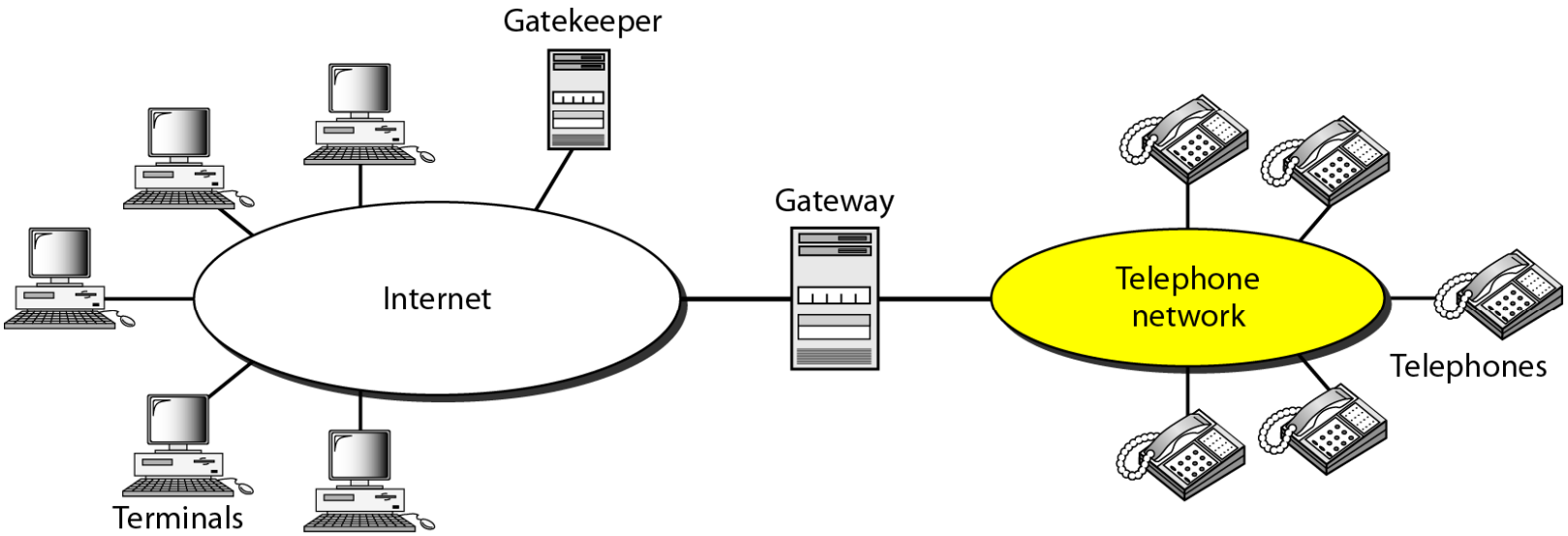


Figure 29.26 *H.323 protocols*

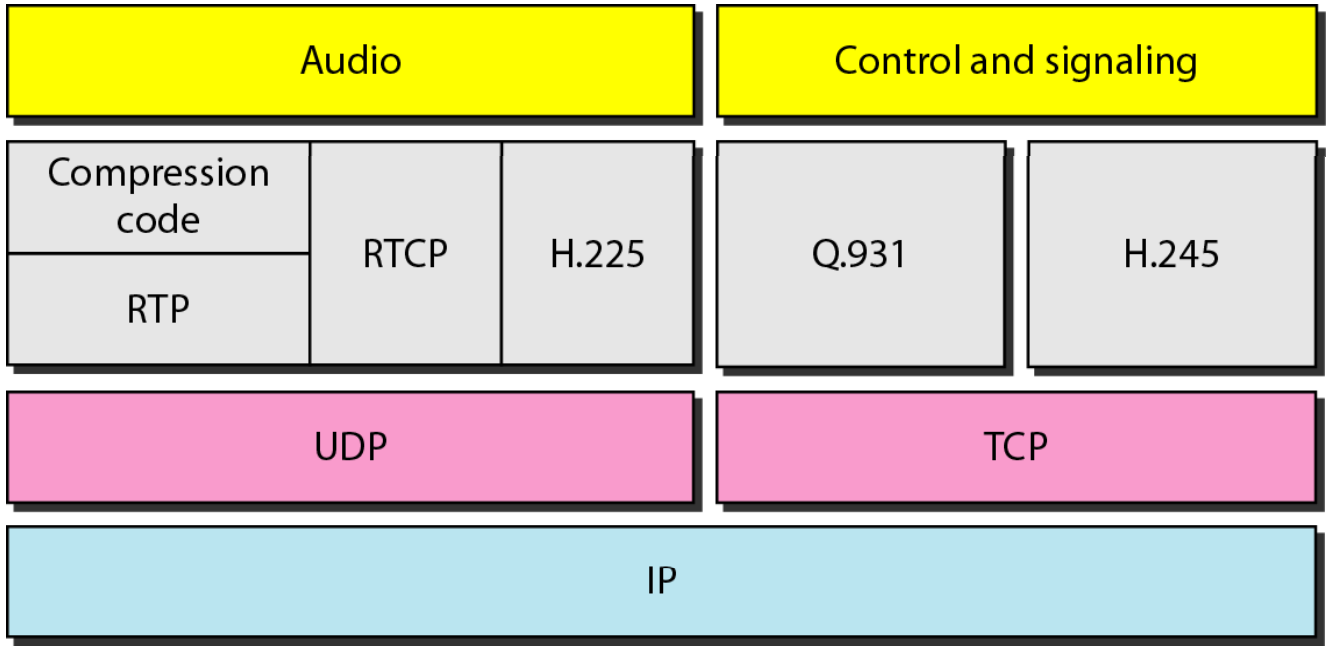


Figure 29.27 *H.323 example*