4. Delivery

Collaborators:
Sr. Lluís Casals Ibáñez
Dr. David Rincón Rivera
Sra. Immaculada Ruiz Vela
Dr. Rafael Vidal Ferré

Dr. Daniel Guasch Murillo

January 2022

4. Delivery

4.1. Internet protocol

4.1. Basic features of IP

Work philosophy IP protocol

- Network layer protocol
- It should be able to use in any host, router, network
- It should be allowed to grow the network without service interruption
- I must admit higher level sessions and message-oriented services

4.1. Basic features of IP

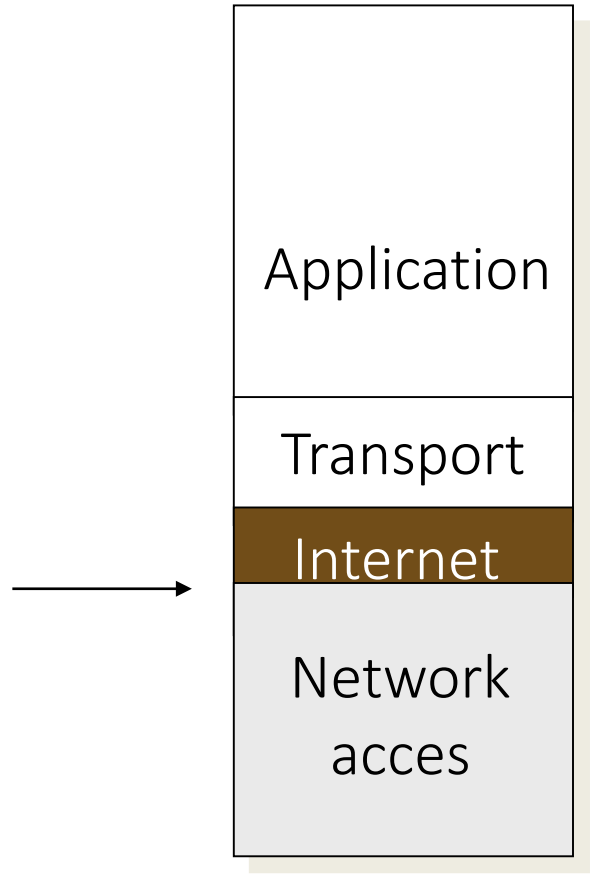
IP (Internet Protocol), RFC791

It is the basis for protocols of TCP / IP family

IP offers:

- link between networks.
- routing (Routing) and freely information between machines on different networks.

package delivery service offline



Datagram

- Minimum transfer unit (PDU)

4.1. Basic features of IP

Service Features

Connectionless

- Each datagram is transmitted independently.

Service without reliability

- There is no guarantee that packets arrive correctly
- They may occur:
  - Lost, duplicated, disorder, ...

Best effort service (will be the best we can).

Reliability is provided by upper levels.

It provides some control functions:

- Through ICMP (Internet Control message protocol)

4.1. Basic features of IP

IP Datagram

The datagram comprises a header and a data field:

- The header contains:
  - IP addresses of the source and destination.
  - And other control information.
- The data field contains the information of the upper protocol

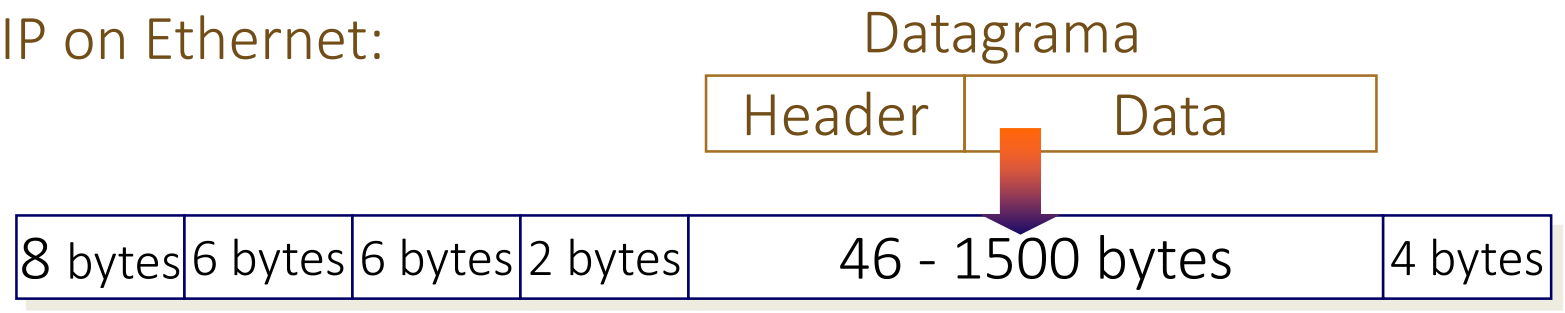
IP datagrama

4.1. Basic features of IP

IP encapsulation

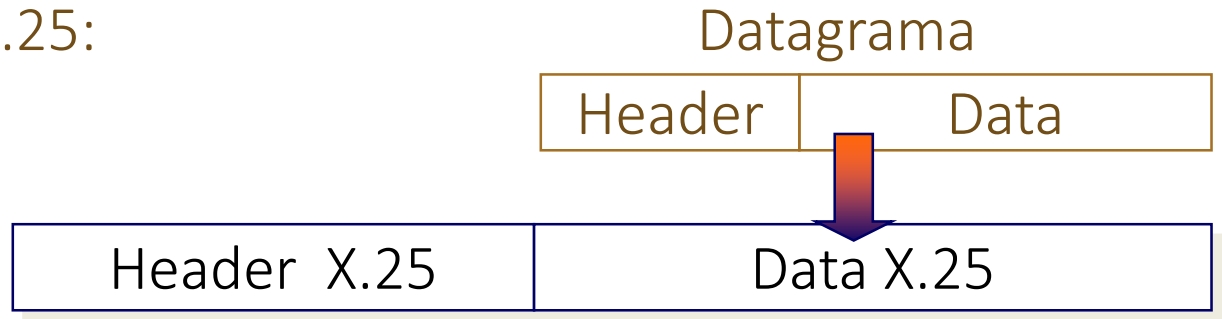
The IP packets are transmitted within the data field of a frame link level:

IP on Ethernet:



There are special cases where IP packets are transported on other levels:

IP on X.25:



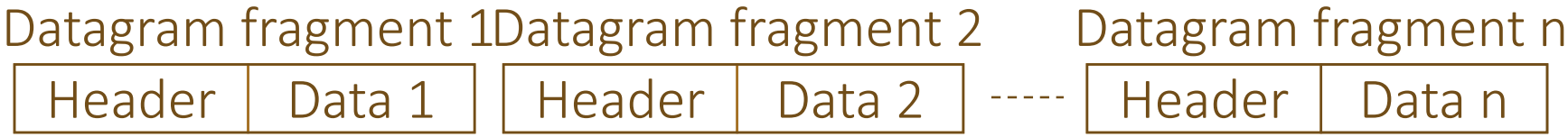
4.2. IP routing function

Fragmentation of IP datagrams

The length of the datagram may be greater than the capacity of the data field of the physical frame:

You have to fragment the IP datagram

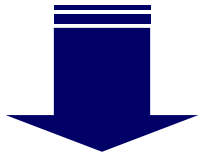
original datagram



4.2. IP routing function

Service Features

The main function of IP is to accept TCP or UDP data, create the necessary datagrams, route them through the network and deliver them to the correct destination



Uses two tools

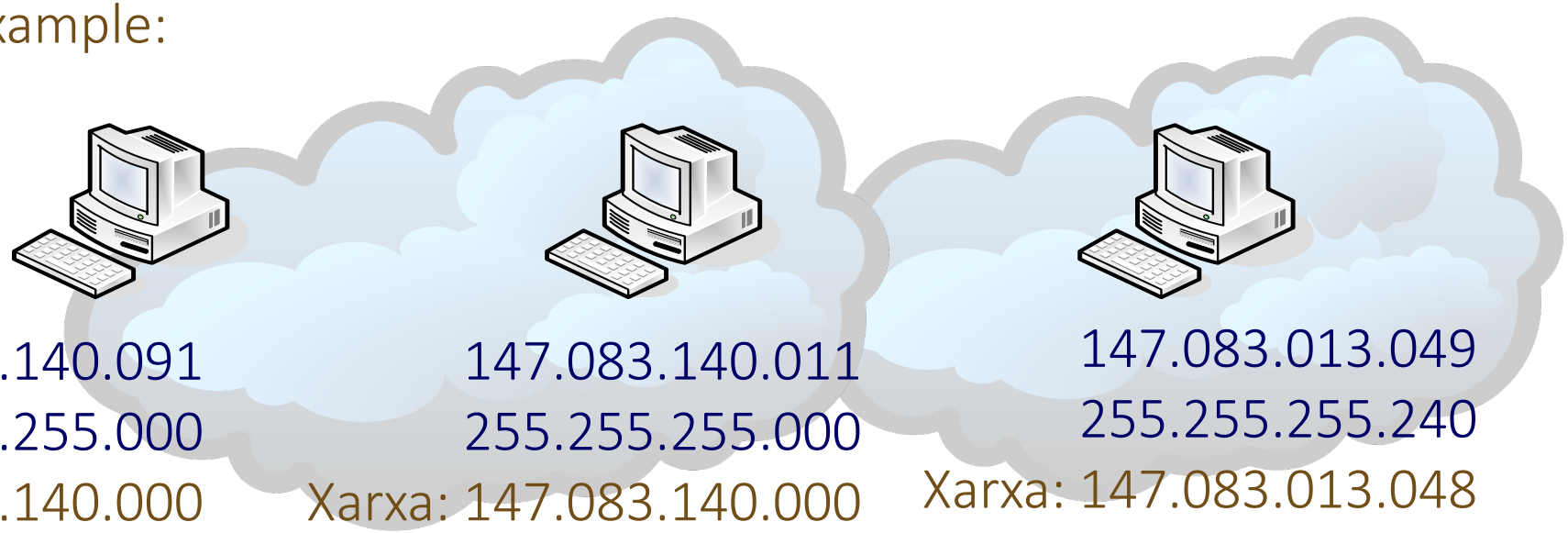
- Subnet mask
- IP routing tables

4.2. IP routing function

Subnet mask

By subnet mask, IP analyzes whether the destination address belongs to the same network as the source address

For example:



4.2. IP routing function

Routing table

Tells IP datagrams as lead to systems that are not on your network

Concept

Do not disclose the full path to the destination.
A IP only needs to know the next-hop address and send the datagram.
IP only defines the structure of the table, not management.
The management of the routing tables is the responsibility of routing protocols.

4.2. IP routing function

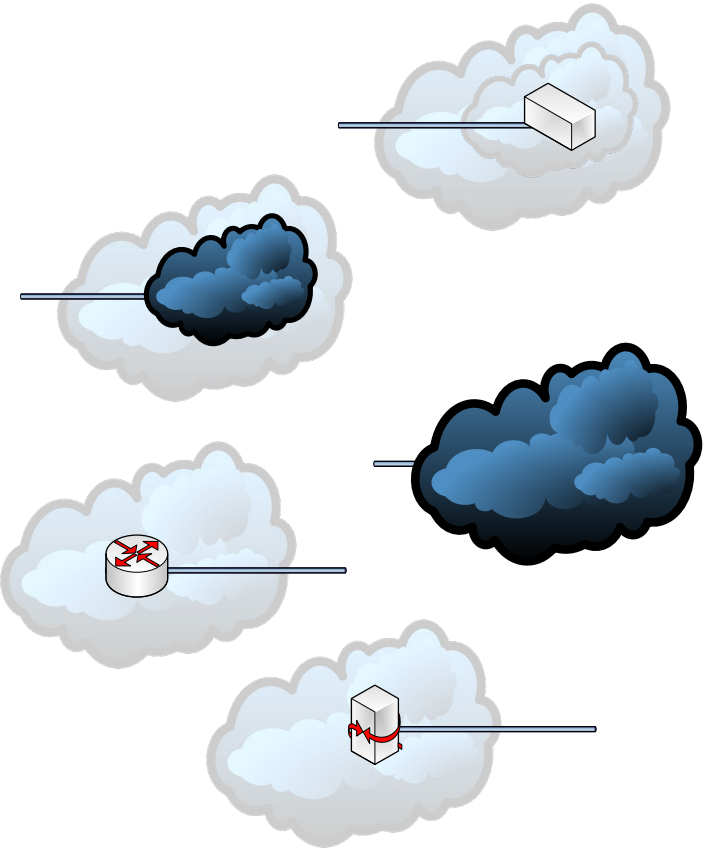
Features of the routing tables

- A station on a network has a routing table
- A host tables are very simple
- Minimum entry must include: default n.n.n
- Tables routers are complex and are managed by two philosophies:
  - Distance Vector: takes into account the number and type of jumps to perform
  - Link Status: create a network map and dynamically evaluates the way

4.2. IP routing function

Search Rules in the routing tables

1. An entry that matches the destination IP address wanted
2. An entry corresponding to the destination subnet wanted
3. An entry corresponding to the destination network is sought
4. An entry for a router is sought
5. The default gateway is used



4.2. IP routing function

Type routes

Static route:

- Those that are predetermined fixed shape. They have little flexibility but generate little traffic routing.

Default route:

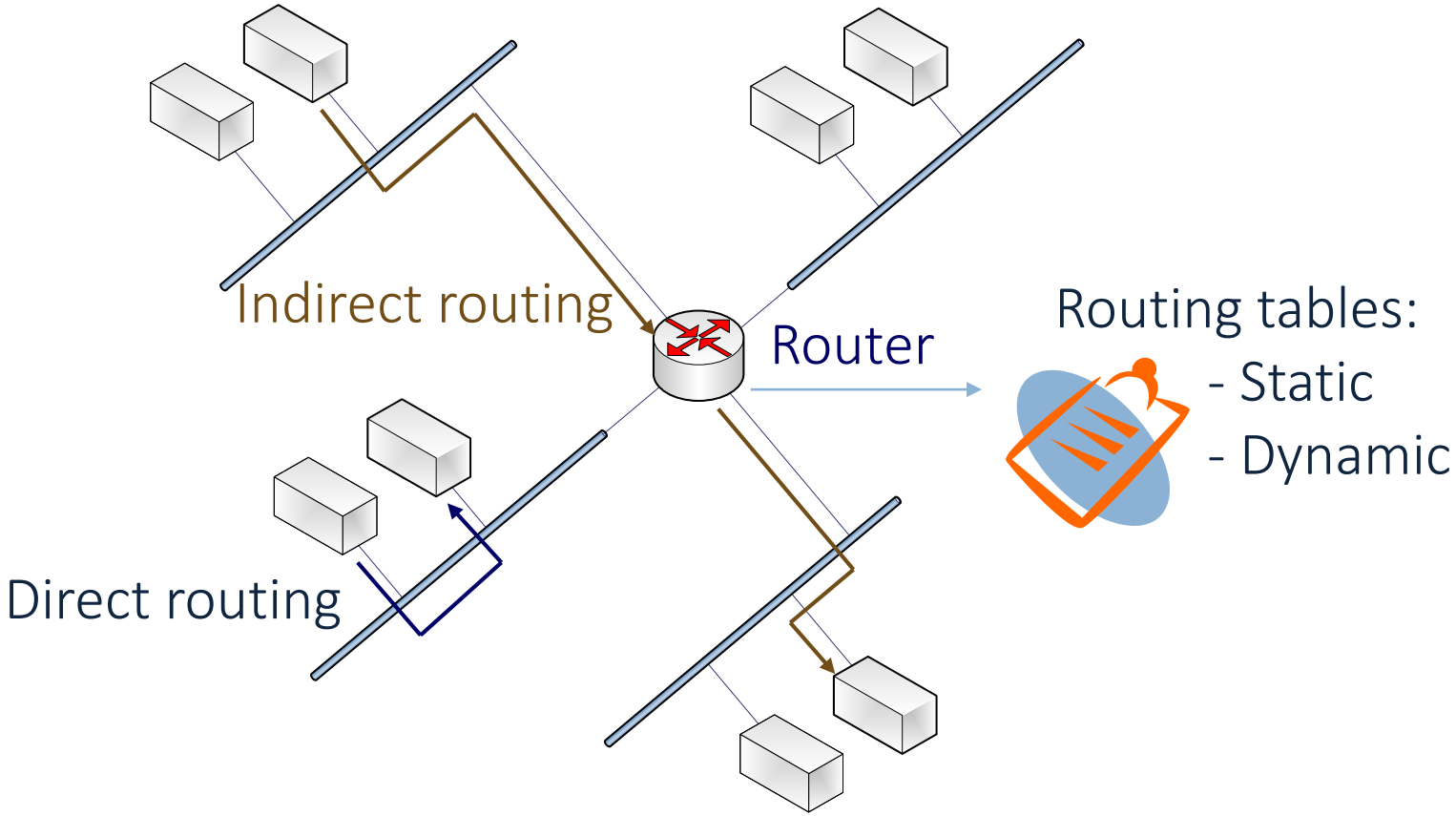
- It would be impractical for a router knew all existing networks. The default path indicates a path where will all packages when a specific route for a particular destination is indicated.

Dynamic route:

- These routes are established according to certain network variables (distance to the destination, path cost, link utilization, etc.). specific protocols are used to exchange information in the routing tables and calculation of the most appropriate routes to each destination.

4.3. Type IP routing

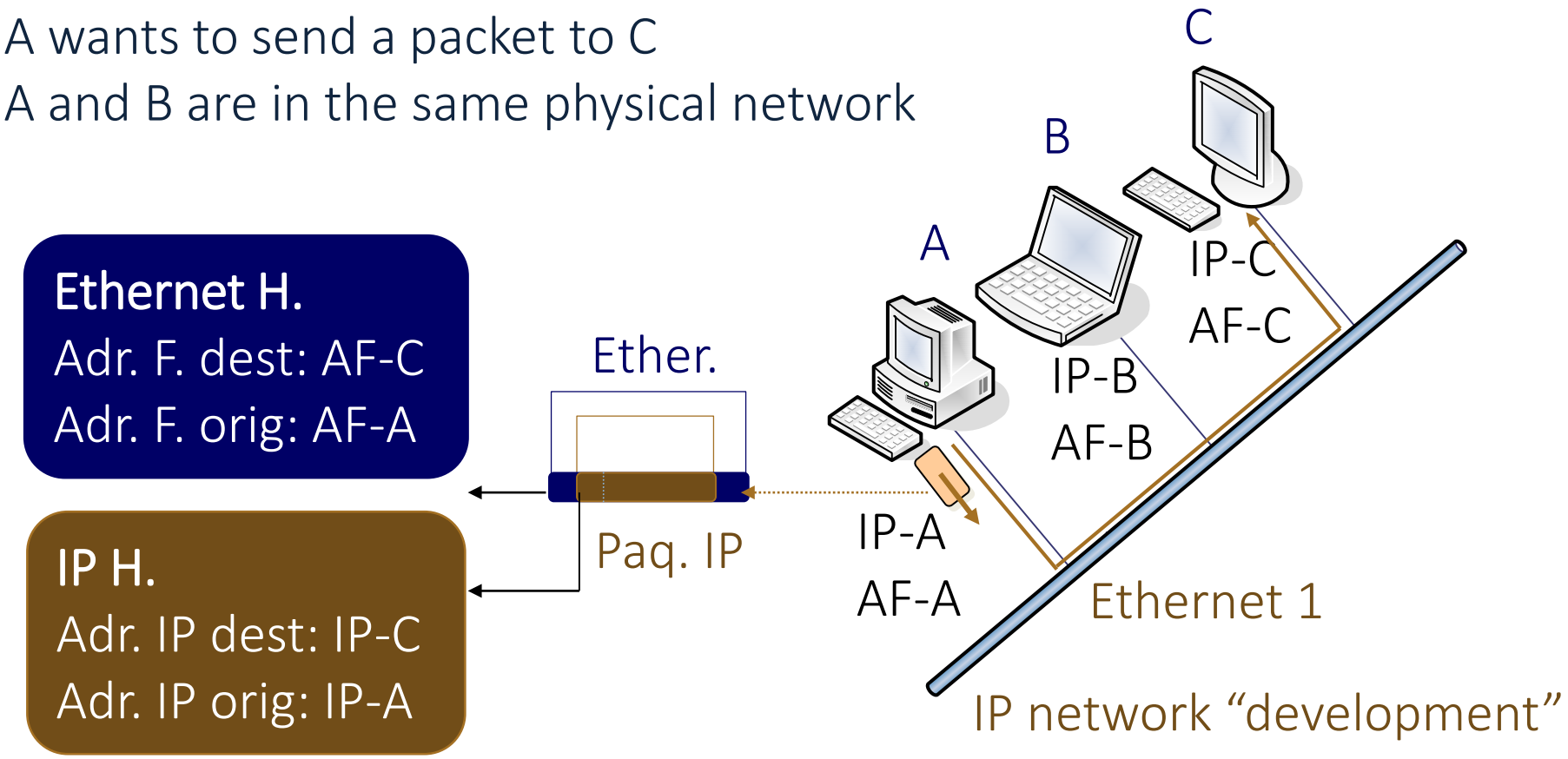
Direct / indirect and static / dynamic routing



4.3. Type IP routing

Direct routing operation

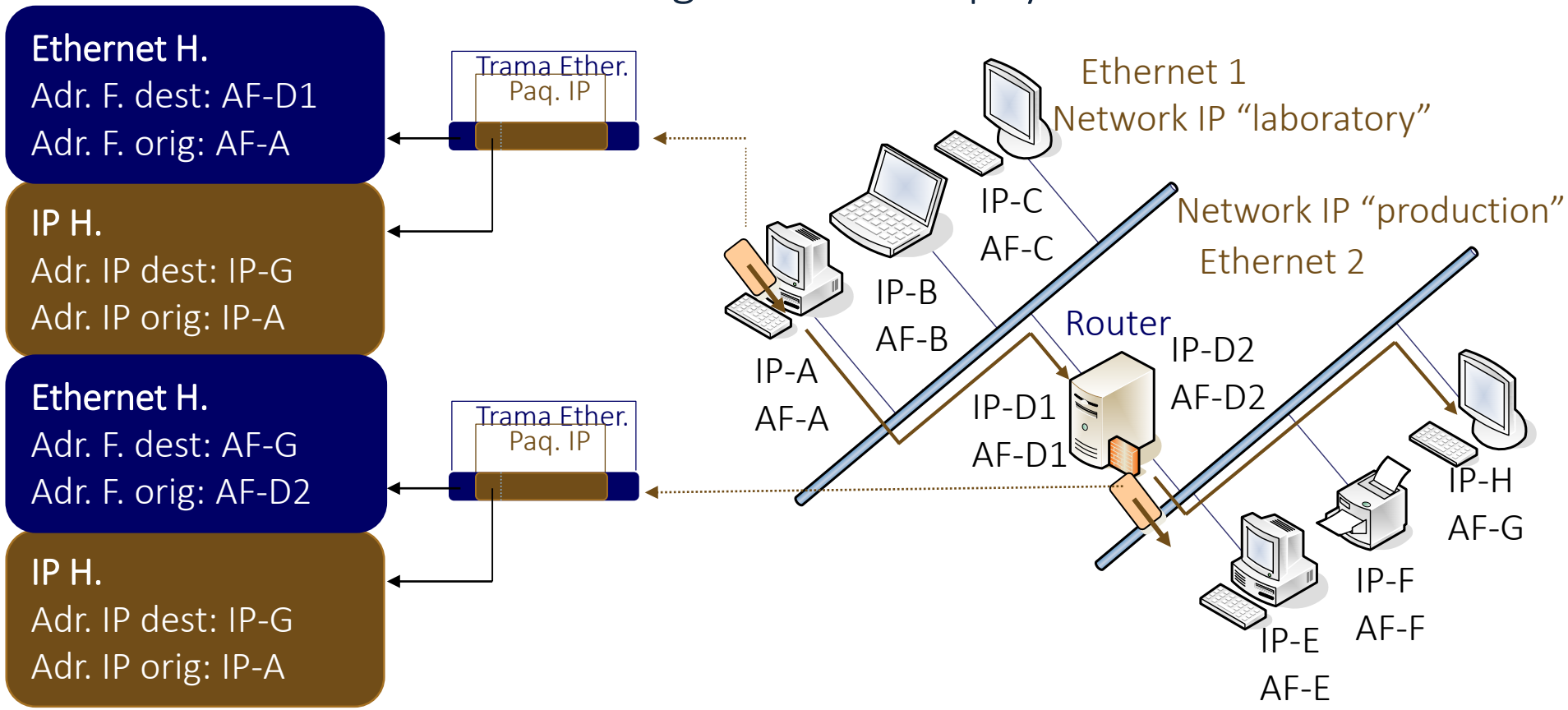
- A wants to send a packet to C
- A and B are in the same physical network



4.3. Type IP routing

Indirect routing operation

- A wants to send a packet to H.
- A and H being on different physical networks



4.4. Fragmentation of IP datagrams

Basic concepts

MTU (Maximum Transmission Unit)

- The plot has a max. Data: MTU
- It depends on the network:

Xarxa física	MTU
Ethernet	1500 bytes
IEEE 802.3	1492 bytes
IEEE 802.5	màx. 4464 bytes
X.25	1600 bytes (may vary for different X.25)
FDDI	4352 bytes
Frame Relay	at least 1600 bytes (normalment)
ATM	9180 bytes (per defecte), màx. 16K - 1

Fragmentation:

- When the package has a length greater than the MTU
- The package is divided into packets with length ≤ MTU

4.4. Fragmentation of IP datagrams

Basic concepts

Fragmentation changes the benefits:

Maximum length of the source → Many fragmentation.

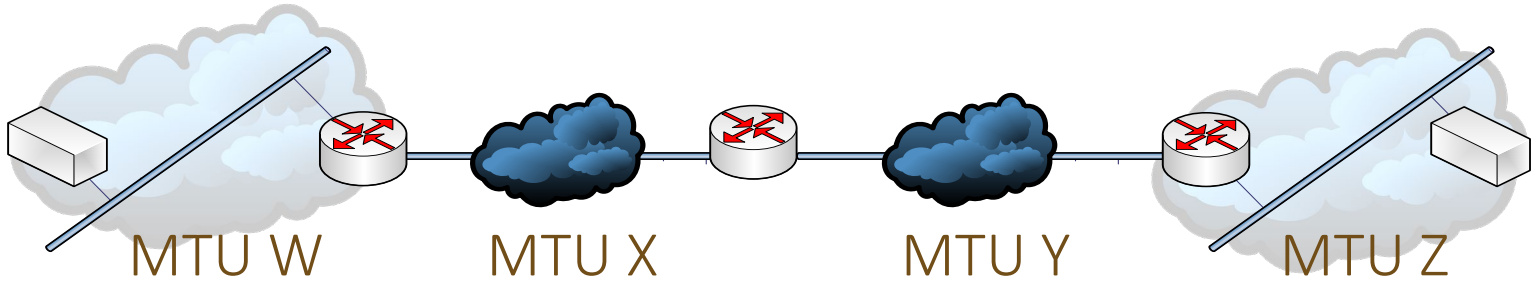
MTU length not to fragment → Efficiency is lost.

Path MTU:

A path MTU is the maximum MTU that does not cause fragmentation.

Mechanism to determine the Path MTU:

Path MTU discovery (RFC 1191), based in ICMP messages.

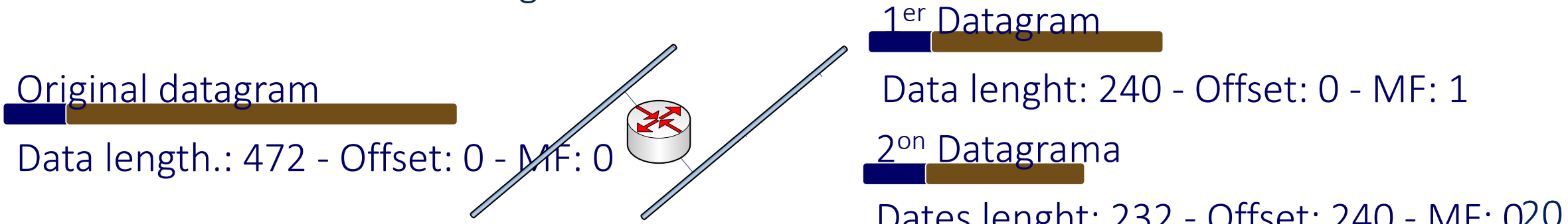


4.5. Fragmentation of IP datagrams

Fragmentation process

When a gateway fragments a datagram makes steps:

- Two datagrams are created and the header is copied to the two
- The data field is divided into multiple byte blocks
- Data blocks are loaded into the respective datagrams
- The "length of the datagram" field is updated
- The flag "MF" the first fragment is updated: set to 1
- The second datagram Offset is modified



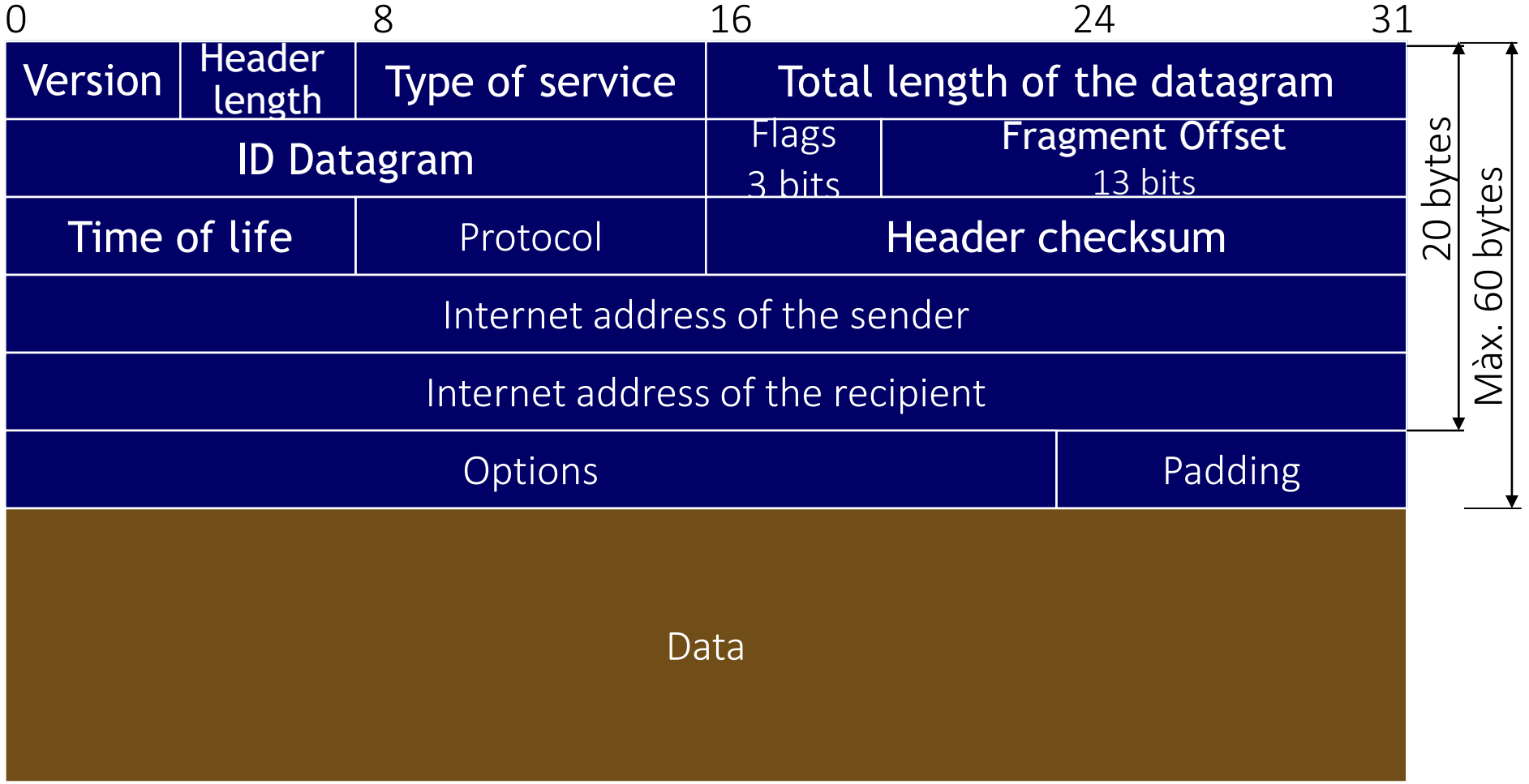
4.5. Fragmentation of IP datagrams

Re-assembling of IP datagrams

The fragments have the same ID, IP source and destination address, and protocolbelonging to the same package.
Fragmentation can occur anywhere on the network. The assembling is done only at the destination.
Problems:
The total size of the original package is unknown.
Memory on routers
Loss of a fragment
A timer is activated when it reaches one of the fragments. If the timer reaches 0 and have not reached all the fragments, the fragments received are discarded and an error message is sent.

4.6. IP datagram format

Structure Datagram



4.6. IP datagram format

Campos "Version" and "header length" datagram

Version (4 bits)

- IP protocol version to ensure that the package is correctly interpreted. Usually it is 4, and the new version is 6.

header length (4 bits)

- Number of 32-bit words of the header, including options.
- If no options worth 5: The minimum header is 20 bytes.
- The maximum length is 60 bytes header.

4.6. IP datagram format

Field "type of service" Datagram

Type of Service (8 bits)

- Specifies how we should treat datagram.
- Defined in RFC 791

- **Precedence**: Importance or priority of the package (8 levels)
- **D T R M**: transport type you want (2 levels):

D = 1 (little delay) T = 1 (high flow) ,

R = 1 (high reliability) M = 1 (economic cost low)

4.6. IP datagram format

"Service type" field of the datagram

Meaning of the bits of TOS (Type Of Service)

DTRM		DTRM	
0 0 0 0	Default	0 1 0 0	Maximizes flow
0 0 0 1	Minimize monetary cost	1 0 0 0	Minimize delay
0 0 1 0	Maximizes reliability	1 1 1 1	Maximizes security

Examples of using TOS bits

	D T R M
TELNET	1 0 0 0
FTP control	1 0 0 0
FTP dades	0 1 0 0
SNMP	0 0 1 0
NNTP	0 0 0 1

Fields "Total length" and "identifier" Datagram

Total length of the datagram (16 bits)

- Total length of the datagram, header + data, in bytes. ? Maximum length 216 = 65,535 bytes
  - But in Ethernet: 1500 Bytes,
  - In IEEE 802.3: 1492 Bytes
  - or in ATM: 9180 Bytes, max. 16KB - 1

Datagram identifier (16 bits)

- No. 16 bits that identifies the datagram. It is assigned sequentially.
  - To control duplication.
  - To facilitate the assembly of the fragments of a datagram.
- If the datagram is fragmented, all fragments have the identifier of the original.

4.6. IP datagram format

Fields "Flags" and "Fragment Offset" Datagram

Flags (3 bits)

- R: reserved bit.
- DF: Do not fragment. The datagram can not be fragmented.
  - Fragmenting if necessary, it is discarded.
- MF: They continue fragments. It is not the last fragment of the package.

Fragment Offset (13 bits)

- Allow to sort the fragments.
- It indicates the position of the fragment in the original datagram.
- It is given in units of 64 bit (8 bytes).
- Except the last, the fragments are multiples length of 8 bytes.

4.6. IP datagram format

Address fields and "Lifetime" Datagram

Internet address of the sender (32 bits)

- Source address of the packet.

Internet address of the receiver (32 bits)

- Destination address of the packet.

TTL: Time To Live (8 bits)

- Specifies the time that the package may remain through the network.
- It is in units of seconds (in practice be a limit max. of life of a package).
- A unit increases (for simplicity) each time it passes a router:
  - when it reaches 0 the packet is discarded.
- Initializes the issuer (usually 32 or 64).

4.6. IP datagram format

Field "protocol" Datagram

Protocol (8 bits)

- Indicates the higher level protocol that is transported in the data field.
- It is coded with a value assigned in RFC 1700:

Decimal	Hexa	Protocol	Descripció
1	01	ICMP	Internet Control Message Protocol
2	02	IGMP	Internet Group Management Protocol
3	03	GGP	Gateway-to-gateway Protocol
4	04	IP	Internet Protocol
6	06	TCP	Transmission Control Protocol
8	08	EGP	Exterior Gateway Protocol
9	09	IGP	Interior Gateway Protocol
17	11	UDP	User Datagram Protocol
29	1D	ISO-TP4	ISO Transport Protocol 4
88	58	IGRP	Internet Gateway Routing Protocol
89	59	OSPFIGP	Open Shortest Path First Protocol

4.6. IP datagram format

Field "Header Checksum" Datagram

Header checksum (16 bits)

- Error checking header (no data).
- It is calculated on each router.
- To calculate this, in the issuer: (RFC 1624)
  - It is set to 0 the checksum field
  - The sum is calculated: 1's complement of 1's complement sum of all 16-bit header
  - The result is saved in the Checksum field.
- To verify, at the receiver:
  - 1's complement sum of the entire header ago: If the result is 0 is correct, but the datagram header is erroneous: the datagram is discarded.

4.6. IP datagram format

Fields "Options" and "Padding" Datagram

Options (variable length)

- This field is carried few packages.
- They provide timestamp, security, and special routing.
- It may take one or more options.
- The structure of the options field has two cases:
  - Case 1: A single byte option type.
  - Case 2: A type of option byte, a length byte option (measured in bytes) and the bytes of option data.
- Subfield structure type of option:
  - **C. F.,** Copy fragment (1 bit)
  - **Class op.,** Option class (2 bits)
  - **N. Opt.,** Option number (5 bits)

Padding: It serves to make the length of the multiple 32-bit header.

4.6. IP datagram format

Subfield "identifier option" Datagram

Option identifier (8 bits)

- **C.F.,** Copy fragment (1 bit):
  - Specifies that the options must be copied to all fragments of the original datagram.
- **Class op.**: class type (2 bits)
  - 0 → control
  - 2 → Debugging and measures
  - 1 i 3 → reserved use
- **N. Opt.**: Option number (5 bits)
  - 2 - Security
  - 3 - Specific route through which must pass the datagram
  - 4 - Timestamp: measures delays between nodes
  - 7 - Record route through which the datagram

4.6. IP datagram format

Subfield "identifier option" Datagram

Some options depending on the type and number:

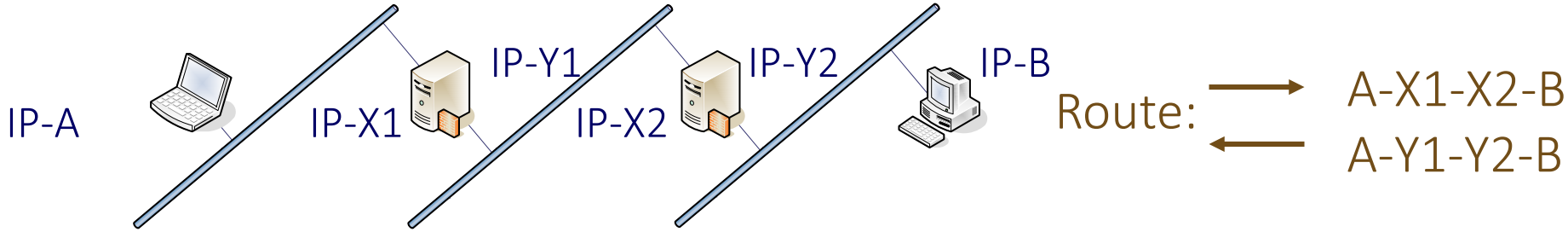
Classe	Número	Longitud	Descripció
0	0	-	Final list of options
0	1	-	Non operation (There is nothing)
0	2	11	Security DoD IP
0	3	variable	Loose source routing
0	7	variable	Record route
0	8	4	Obsolet
0	9	variable	Strict Source Routing
2	4	variable	Timestamp

4.6. IP datagram format

Source routing options Datagram

Source routing:

- The route packets must follow is given by the source
- Des packets traveling destination to the source must use the same route packets going from source to destination.
- Type: Strict (strict) and off (Loose).
- Problem

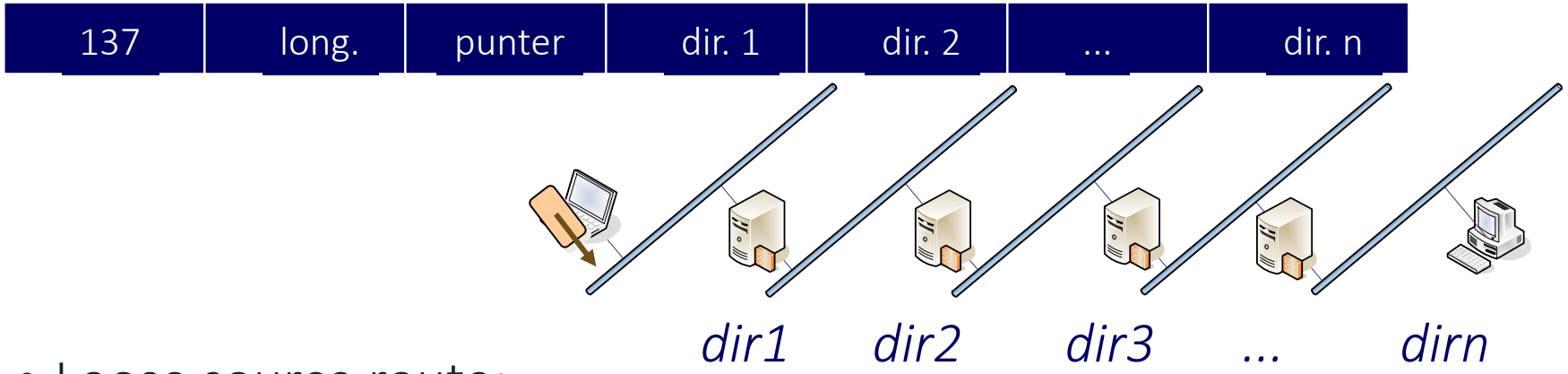


- You can not use the route description given by A.
- Routers modify the input addresses by output.

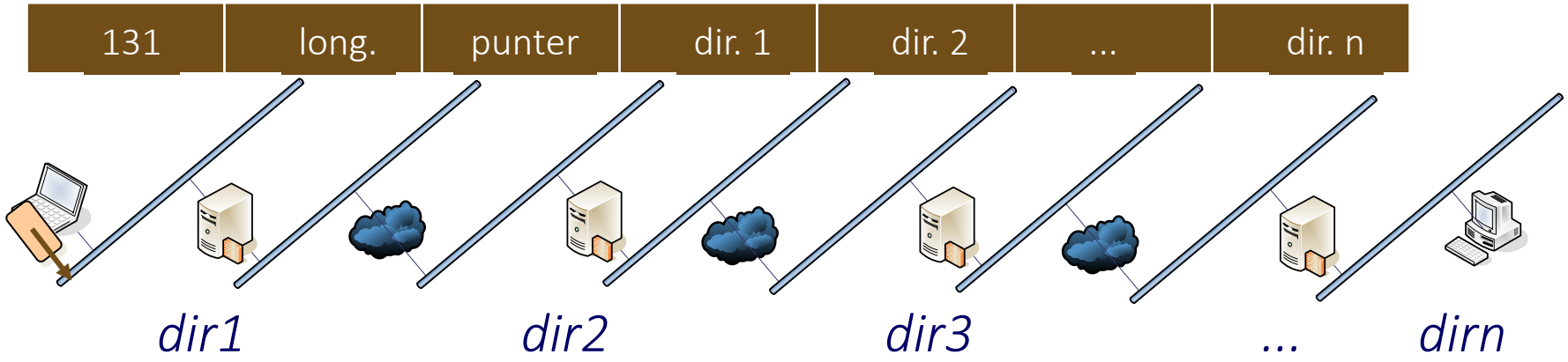
4.6. IP datagram format

Source routing options Datagram

- Strict source route:



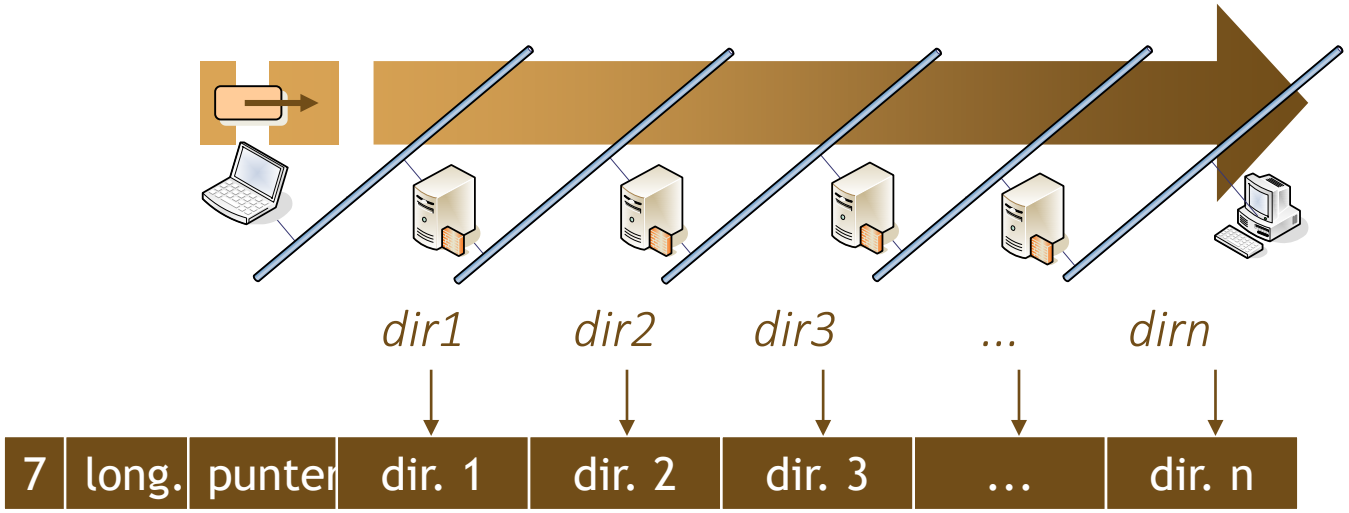
- Loose source route:



4.6. IP datagram format

Source routing options Datagram

- Record route: addresses are added



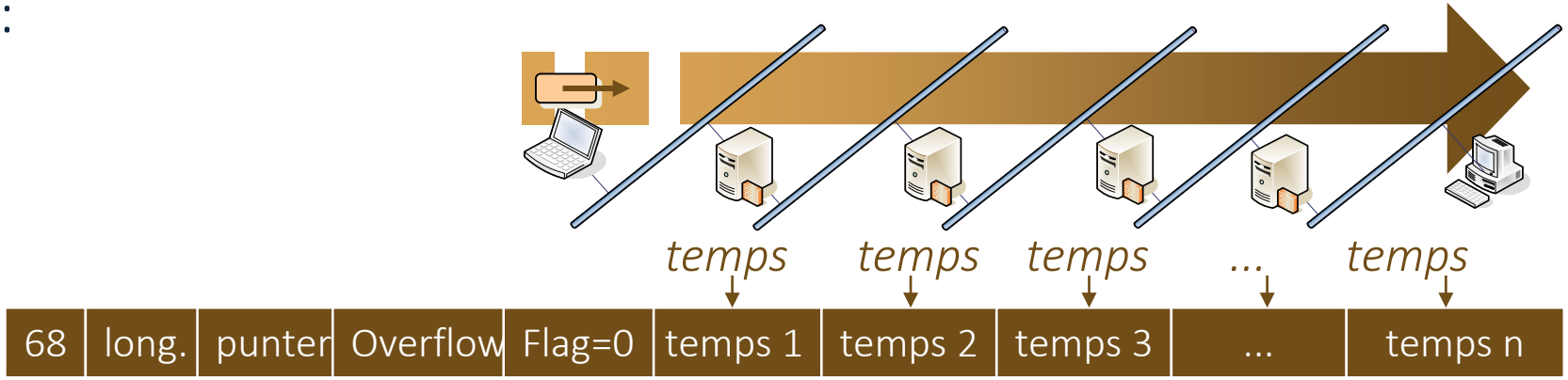
pointer (in bytes): indicates the position at address. Start with the fourth byte and increases by four.

If pointer> length: You have used all directions and is headed by the destination address.

4.6. IP datagram format

Source routing options Datagram

- Timestamp:



- Flag (4 bits): type of format

  0 → In each jump the time is saved in the reserved space and pointer is increased in 4.

- Overflow (4 bits) is the name of IP modules that can not register timestamps due to lack of space.

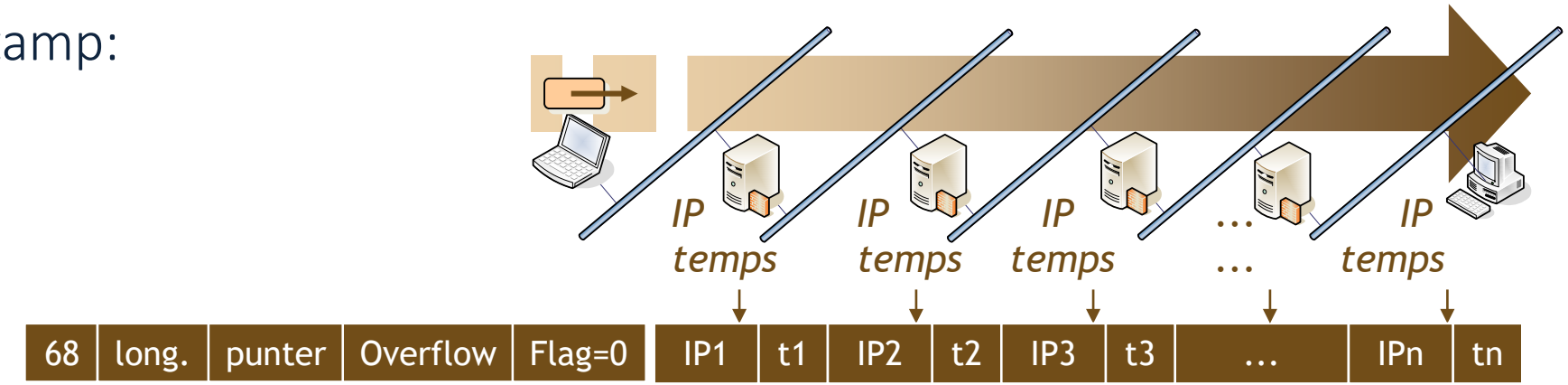
  If the reserved space is exceeded Overflow field is incremented by 1.

  If the Overflow field is depleted (> 15) the datagram is discarded.

4.6. IP datagram format

Source routing options Datagram

- Timestamp:



Timestamp. Flag = 1 and 3

1 → In each jump the time and address of the router is saved. space for two golf reserves and increases in 8 pointer.

3 → The source indicates which nodes can record the time. If the router founds its address on the list adds the timestamp.c

4.7. Internet Control Message Protocol

Problems associated with IP protocol

Protocol IP → Unreliable
Connectionless

- A control mechanism is needed:
  - Why a datagram has not been able to deliver?
    - The target machine is not connected wing network
    - The timer has expired
    - Network congestion
  - Indication of errors occurred in the treatment of datagrams
  - Discovery of new routes
  - A router does not have enough buffer to store packets

4.7. Internet Control Message Protocol

Fundamentals of ICMP protocol

It was initially developed because the routers inform the causes of error in the delivery of packages.

The ICMP protocol does the most reliable IP protocol, only reports errors to the source machine, but not the intermediate nodes.

- Reliability is achieved with higher levels protocols.

The ICMP error notification messages goes to the source host (who sent the package that causes the error).

- Intermediate routers have no knowledge of errors and can not act.

ICMP packets can also have errors. In this case no other ICMP packet is generated (to prevent recurrence).

4.7. Internet Control Message Protocol

Encapsulation of ICMP messages

ICMP messages travel in the data field of the IP protocol, but not a high level protocol.

Usually it considered as a part of the IP level.

The recipient is the IP module, not the origin or destination user.

The ICMP messages can be:

- Error Messages (used by routers)
- Query messages (used by hosts)

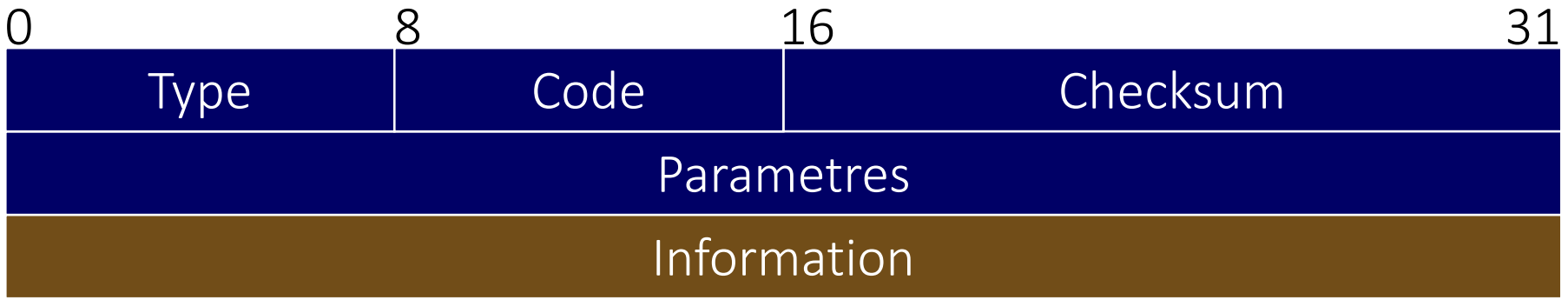
Conditions of generation of ICMP messages

An ICMP error message is never generated as a response to:

- Another ICMP error message (except for ICMP query messages).
- A packet destination address broadcast or multicast.
- A packet sent as a broadcast to the link layer.
- A fragment of a packet (not the first case).
- A package which the source address does not define a single host (source address can not be 0, Loopback, broadcast or multicast).

4.8. ICMP messages

Format of ICMP messages



- **Type:** ICMP message type. There are 15 possible messages.
- **Code:** Identify any additional condition for each type of ICMP message.
- **Checksum:** To protect the ICMP message errors. ICMP message is calculated on everything and uses the same algorithm for the IP header.
- **Parameters:** Message parameters.
- **Information:** Header and first 8 bytes of the datagram that caused the ICMP message generation.

4.8. ICMP messages

ICMP messages type

0 - Echo Response: To test if you can get a machine (ping)

3 - not acceptable Destination

4 - Flow control (Source Quench): a memory overflows

5 - Rerouting: to indicate that there is a better route

8 - Echo Request (ping)

11 - time exhausted Datagram: circular routes or too long

12 - Problem in a parameter Datagram

13 - Request for timestamp: time control of the route

14 - Response timestamp

15 - Information request (obsolete)

16 - Information Reply (obsolete)

17 - Request for the subnet mask

18 - Response subnet mask

Treatment of ICMP messages

Destination not acceptable:

- ICMP deliver the message to the transport layer.
- The next action will depend on the cause of this error.

Rerouting (redirect):

- The host must update the routing table.

Source quench:

- Deliver the message to the transport layer or an ICMP processing module.

Exhausted time:

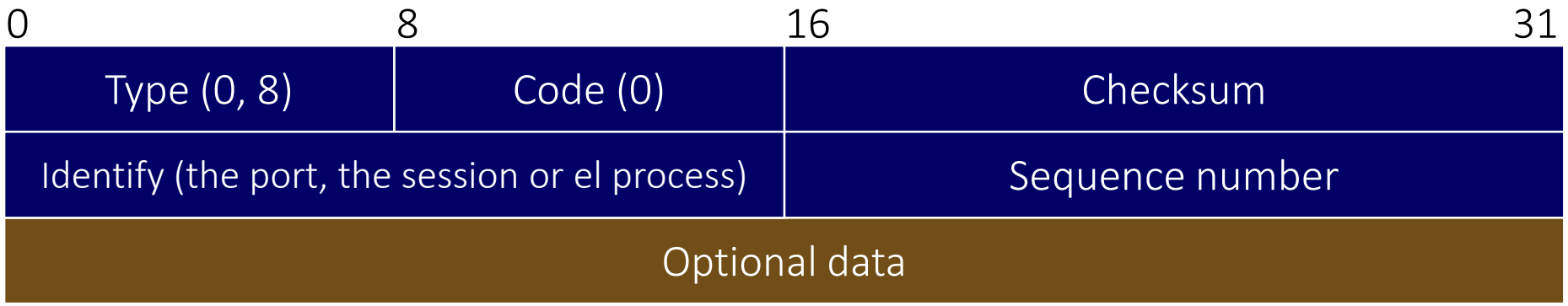
- Deliver the message to the transport layer

Incorrect parameters:

- Deliver the message to the transport layer; optionally notify the user.

4.8. ICMP messages

ECO messages



Type: answer → 0, request → 8

Identify: To identify which is the origin within the host origin.

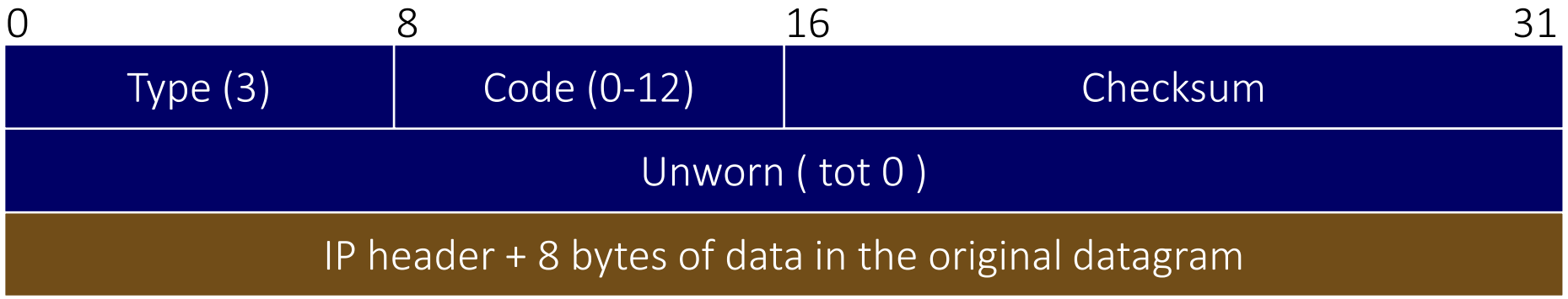
Optional data: The originator can put data that fate will return in response ECO.

Sequence number: ECO to identify a single burst messages (which have the same identifier)

Used by the ping service.

4.8. ICMP messages

Error messages: destination not reachable



By routers and hosts:

- **Routers:** not known network can not fragmenting, host not available, etc.
- **Hosts**: IP protocol package is not available, non-assumable habour.

4.8. ICMP messages

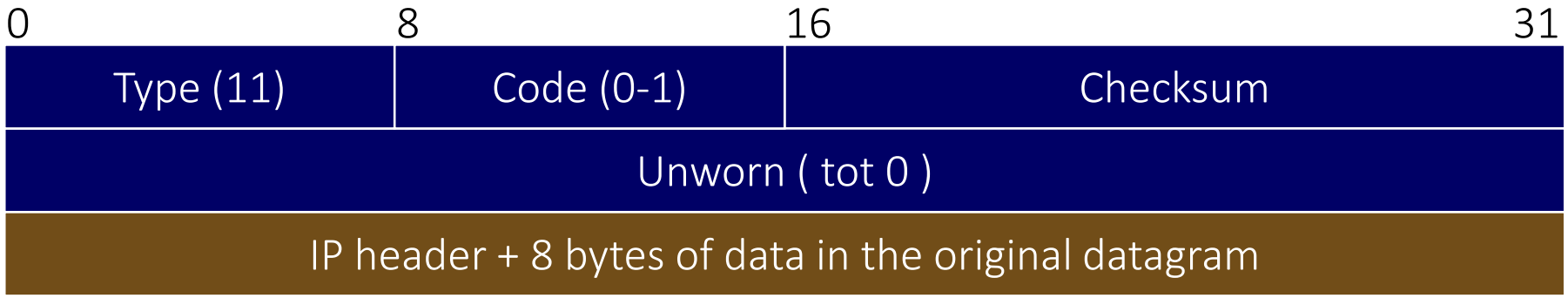
Error messages: destination not reachable

- The code camp identify the error:

0 - Network unreachable
1 - Host unreachable
2 - Protocol unreachable
3 - Port unreachable
4 - Fragmentation needed and Do Not Fragment flag is set
5 - Source route failed
6 - Destination network unknown
7 - Destination host unknown
8 - Source host isolated
9 - Communication with destination network administratively prohibited
10 - Communication with destination host administratively prohibited
11 - Network unreachable for type of service
12 - Host unreachable for type of service

4.8. ICMP messages

Error messages: Time out



Code: 0 – Time to Live has been exhausted
1 – It is exhausted timer assembling

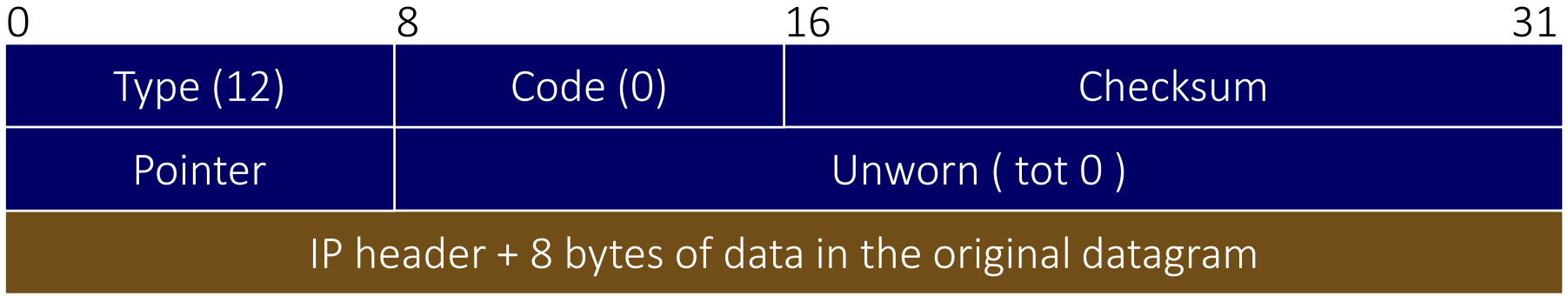
Because circular or excessively long routes.

When the life time of a packet is finished, the router discards it and sends an ICMP error message.

Straining the timer in the reassembly of a datagram (sent des host destination).

4.8. ICMP messages

Error messages: Incorrect parameters



Code: 0 - The pointer indicates where the problem is.
1 - Military applications: lack an option; the pointer is not used.

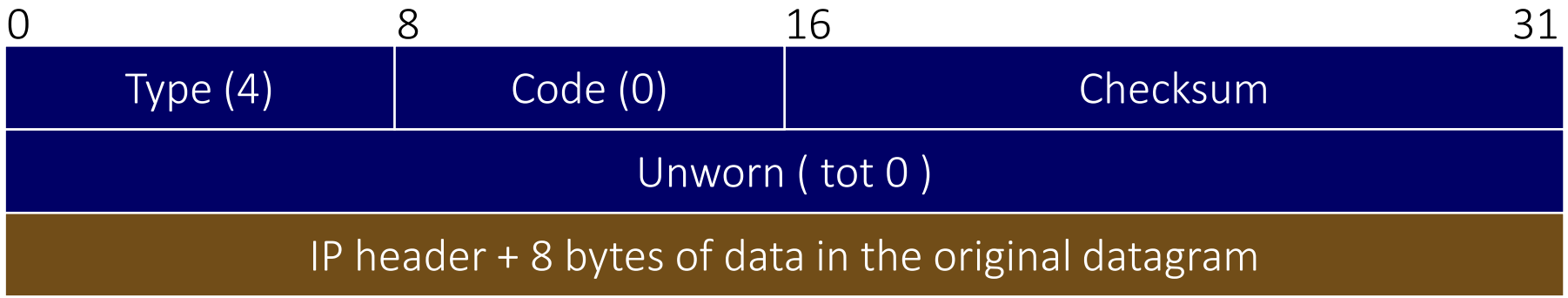
Due to a problem with the datagram header.

In datagram is discarded and the ICMP message is sent.

The pointer indicates the byte in the header where the error.

4.8. ICMP messages

Messages flow control: Source Quench



Send by routers and hosts that are faster than they can process data.

If the input buffer is filled datagrams will be lost.

When a packet is lost is sent an ICMP so it can be forwarded.

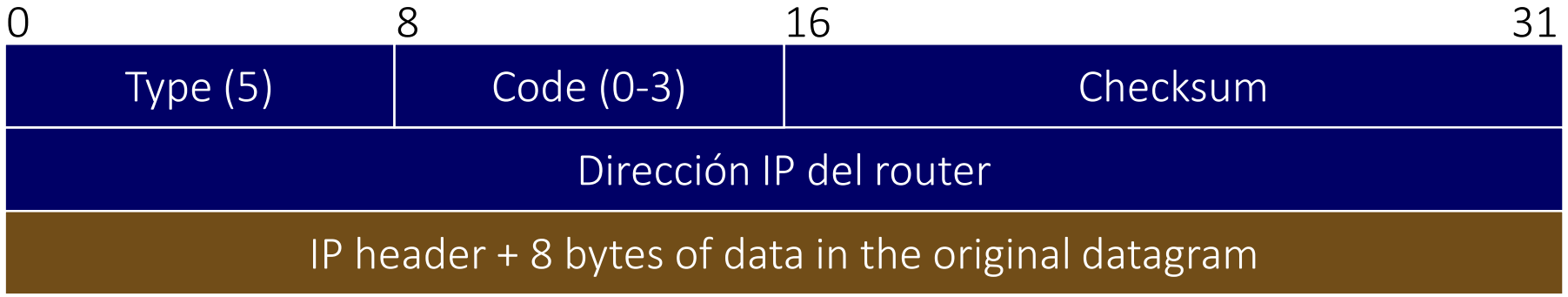
When an ICMP message is received from this source Type sends packets more slowly.

Later, he turns to increase the pace slowly.

Message Type This practically not used.

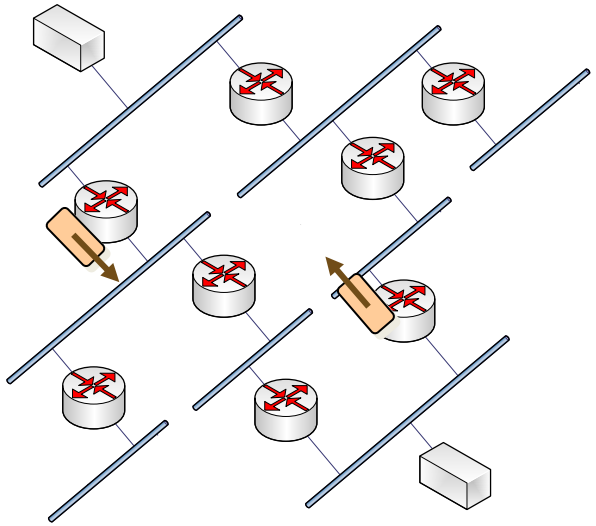
4.8. ICMP messages

Routing messages: redirect (rerouting)



Only routers send.

Report that there is a better route.



4.8. ICMP messages

Routing messages: redirect (rerouting)

When a dynamic routing protocol is used, routers learn of new routes but not the hosts.

The routers send information to the hosts to update the default router entry in the routing table.

The hosts rely on routers to maintain routing information.

Codes ICMP redirect message (Rerouting):

0 → Datagram forwarding the same network (obsolete)

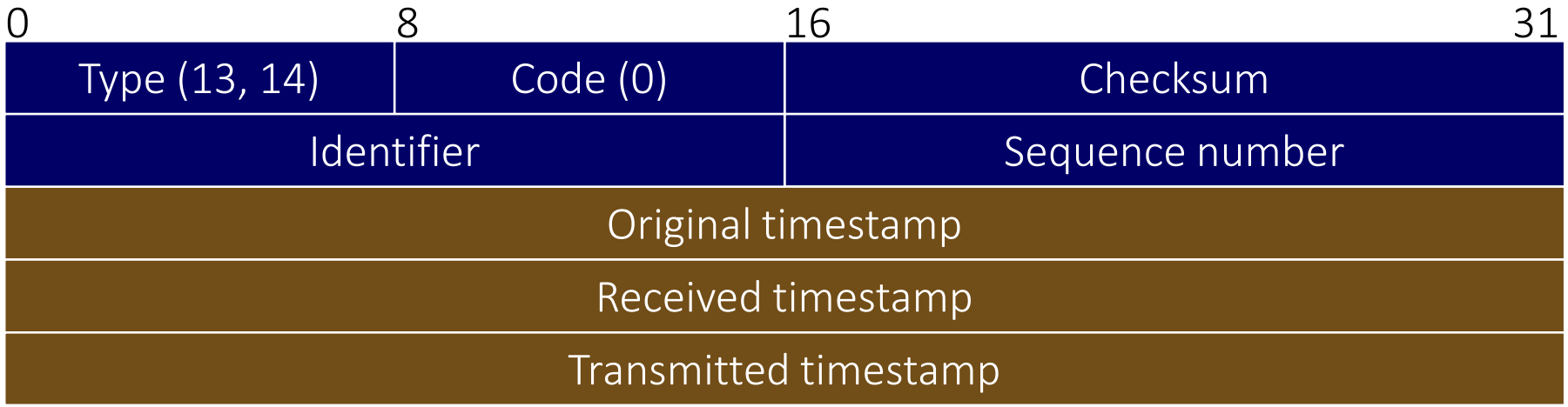
1 → Redirect datagrams on the same host

2 → Redirect datagrams the same type of service and network

3 → Redirect datagrams the same type of service and host

4.8. ICMP messages

Routing messages: Brands of time



Code: 13 - message; 14 - answer

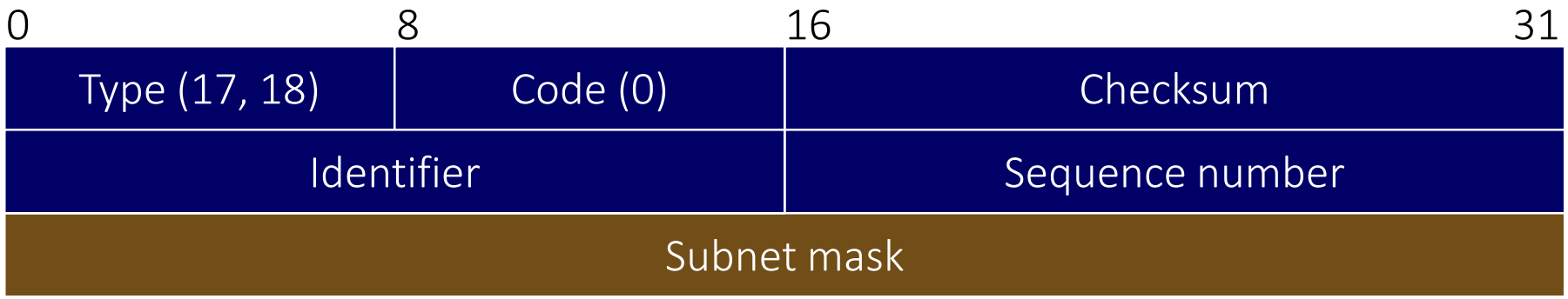
independent machines → unsynchronized clocks

The message timestamp used to synchronize machines and estimate the transit time of the package.

Problem: The transit time of a packet can vary greatly from one attempt to another.

4.8. ICMP messages

Routing messages: Getting mask



Code: 17 - Request
18 - Answer

When the host does not know which subnet mask is used in your subnet the can ask a router (or server mask).

The request can be sent to a router directly, if the address is known, or can be, if not, make a broadcast to the network.

4.8. ICMP messages

Routing messages: Discovery route

Routers periodically send information so hosts can discover new routes.

Hosts can also request this information.

Messages can be sent to the addresses:

Multicast, all systems:	224.0.0.1
Multicast, all routers:	224.0.0.2
Broadcast:	255.255.255.255

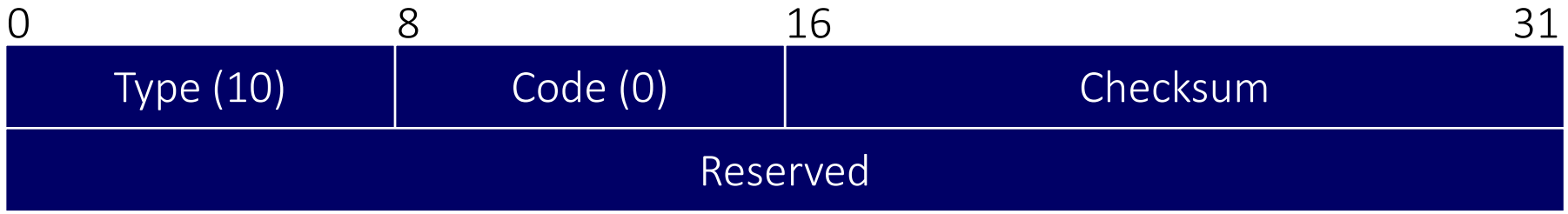
Need for a default router → File → No dynamic procedure → ICMP messages of best routes

- Some hosts interpret routing protocols
  Router Discovery Protocol (RDP)

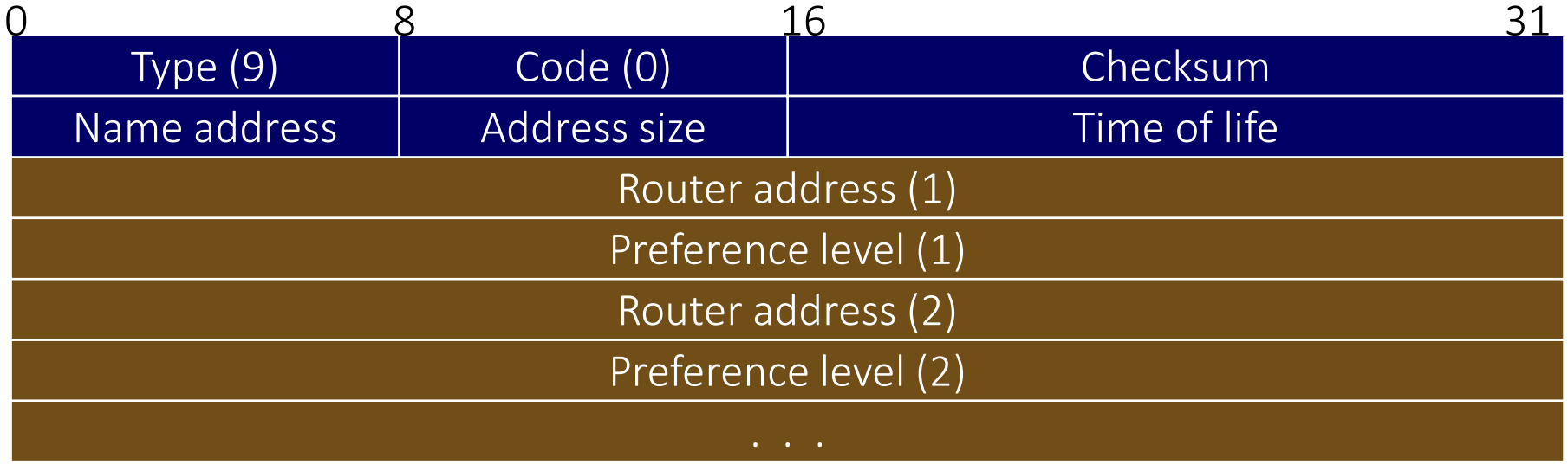
4.8. ICMP messages

Routing messages: Discovery route

Request



Announcement - answer



4.8. ICMP messages

Routing messages: Discovery route

Name address:

- How many addresses informs the message.

Size address:

- Few 32 bit words are used to describe a direction. Currently he is always 2.

Life time:

- Time during which the addresses can be considered valid

Router address (n) :

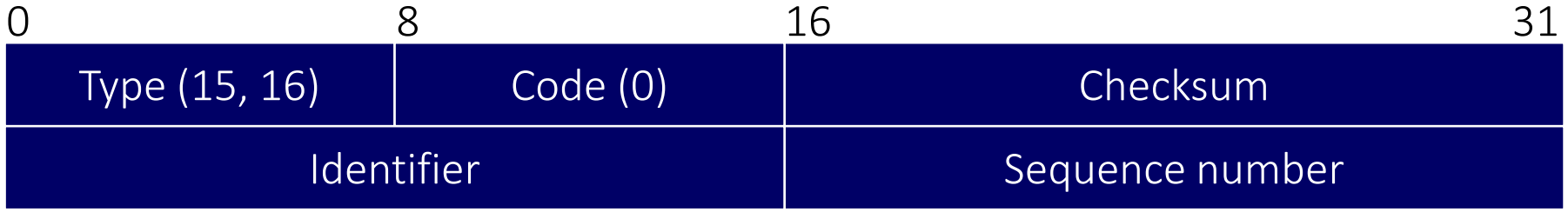
- N router IP address of the interface through which sent the ad.

Preference level (n):

- The higher value is the most recommended is the use of this router.

4.8. ICMP messages

Information Messages



Code: 15 - Request
16 - Answer

These messages are considered obsolete.

They were used because certain hosts could get your IP address when operated. RARP (or other protocols) are currently used.

4.9. Practical examples

Useful commands in IP environments

Use the hostname function to get the name of a host.

Use the ping function to know the IP address of a host.

Lookup use the function to obtain DNS server information.

Use the netstat -r or netstat -nr function to know the host routing table.

I use the netstat -a netstat to know the active TCP / IP host connections.

Use the netstat -s function to obtain information from ICMP messages circulating on the host.

Use the tracert function to discover the path that an IP packet would follow to destination

4.10. IP version 6

General concepts of IP version 6

Addressing problems → IPng (next generation) IP version 6

IPv6 is defined in RFC 1883, RFC 2460

Improvements over version 4:

- More capacity Address : **32 bits** → **128 bits**
- Simplified header format: unnecessary or redundant fields
- It facilitates the configuration and location of routers
- Best extensions and options
- Type concept traffic
- Security: authentication, integrity, confidentiality

4.10. IP version 6

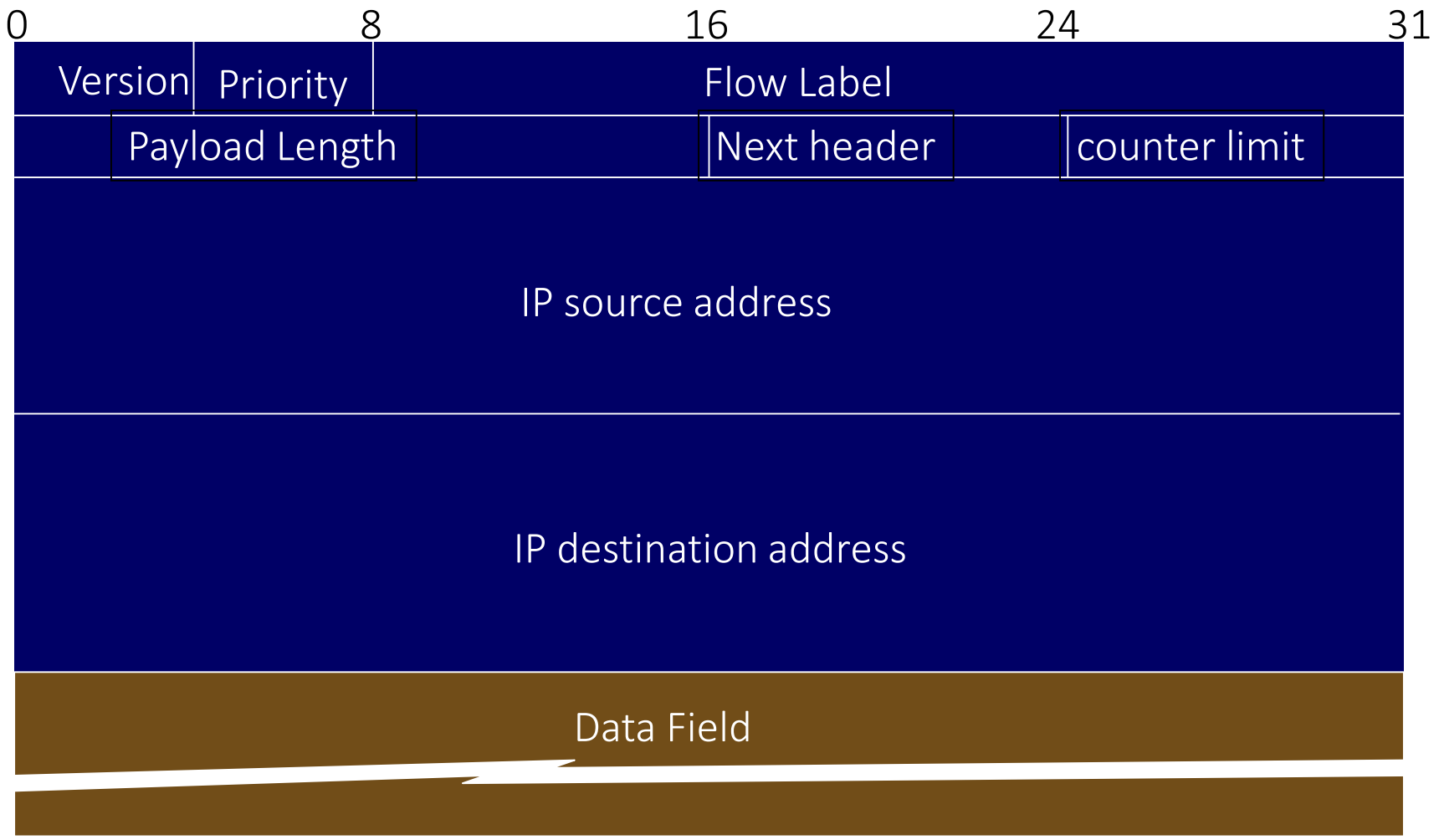
IP version 6 format package

Simpler format

- No checksum
  - Protecting make the upper and lower protocols
  - It is assumed that the link is "good" (fiber, etc.)
- Fragmentation is removed
  - To streamline the protocol
  - If necessary done in source.
- Options are not included
  - Extension headers

4.10. IP version 6

IP version 6 format package



4.10. IP version 6

IP header format version 6

Version (4 bits)

- Identifies the version

Priority (4 bits)

- Transit Priority Order
- Two Type of transit
  - 0-7 applications that allow congestion control (eg. TCP)
  - 8-15 applications that do not support congestion control
    - The network can be discarded without affecting the integrity of the information

4.10. IP version 6

IP header format version 6

Priority values (higher ⇒ highest priority)

- 0 transit uncharacterized
- 1 transit filler (news, ..)
- 2 Transit unattended data (e-mail)
- 3 reserved
- 4 data traffic served, file transfer (NFS, FTP ..)
- 5 reserved
- 6 interactive traffic (Telnet, XWindows, ..)
- 7 Internet traffic control (routing, SNMP, ..)

4.10. IP version 6

IP header format version 6

Flow label (24 bits)

- Identifies the type of traffic, always the same destination
- faster routing (only the first packet is processed)
- Resource Reservation

Payload Length (16 bits)

- With 16 bits ⇒ 65535 bytes
- larger packages ⇒ Jumbograma
  - Defined by extensions

Next header (8 bits)

- Indicates whether another header, and type

4.10. IP version 6

IP header format version 6

Hop limit (8 bits)

- Same function as TTL
- But it is a “real”
- counter

Source and destination addresses (128 bits)

- Addresses 665.570.793.348.866.943.898.599
  - 6,7 x 10^{23} addresses

    With an efficient allocation can have 1564 addresses per m2 (Earth)

Extension of IP headers version 6

For more complex tasks (fragmentation information, routing) Special headers are used.

Extension headers

- Hop by Hop: It contains IP options for each system in the path of the datagram
- Routing: It allows the source routing the datagram, similar to IPv4
- Fragmentation: fragmentation information sent by the source to the destination. Intermediate nodes do not fragment.
- Encrypted data: It ensures that the datagram has not been altered during transmission
- Authentication: data origin authentication
- Target Options : Two types of headers to define

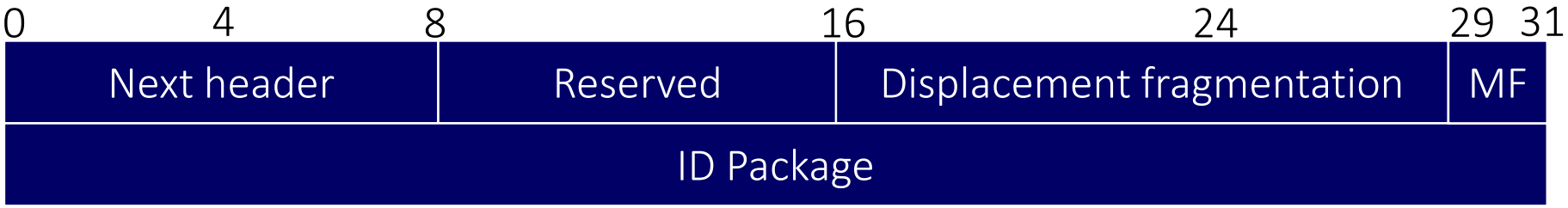
Extension header: fragmentation

Fragmentation information sent by the source to the destination.

- Intermediate nodes not fragmented, fragmentation is restricted to the source.
- Path MTU discovery process prior to sending the package to end to end fragmentation.

Each fragment must be a multiple of 8 bytes.

The MF bit indicates if there are more fragments



Extension header: fragmentation

Packet Identifier

- Identify fragments belonging to a package
  - Identifier 32-bit to adapt to high-speed networks.

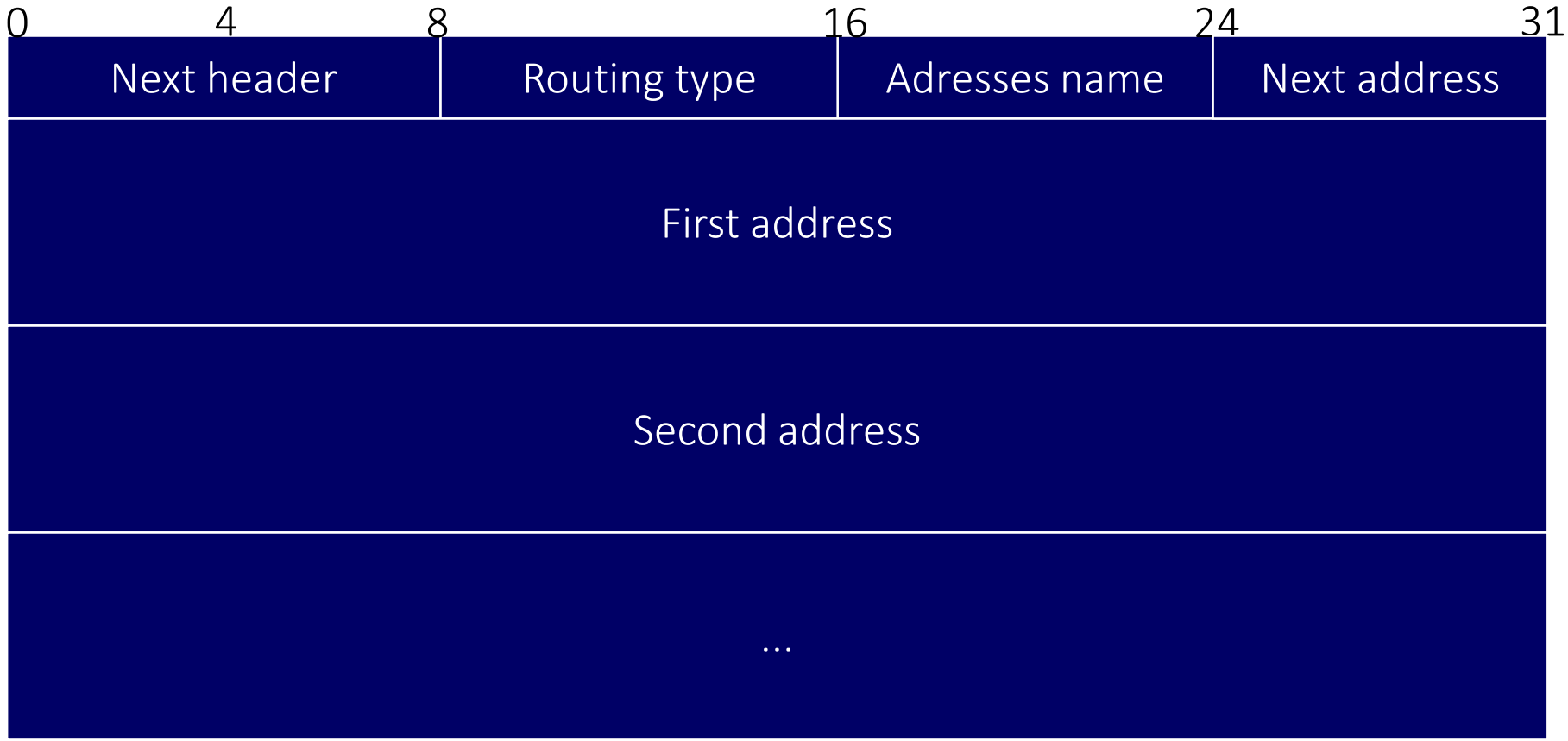
What if there is a change of route?

- If you change the path MTU, the router must implement fragmentation takes an IPv6 over IPv6 tunnel to transport the fragments of the original package.

4.10. IP version 6

Extension header: source routing

It is similar to the source routing options IPv4.

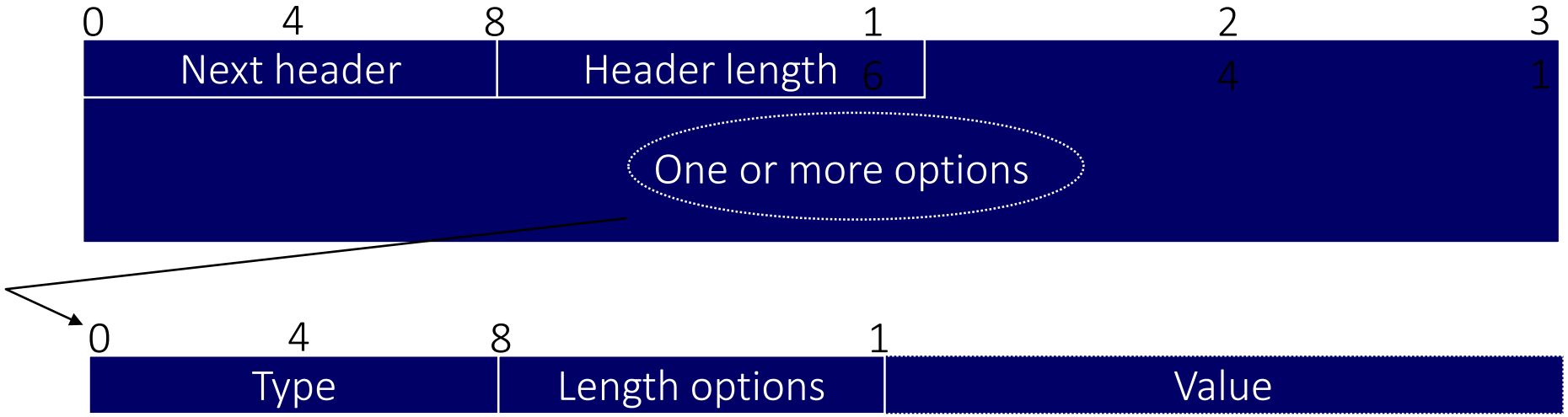


4.10. IP version 6

Extension header: IPv6 Options

2 additional header extensions are defined to fit any type of information not included in the header information already defined.

- Hop by hop Extension Header: Options interpreted to each jump.
- End to End Extension Header: Performed at the extreme end options



4.11. IPsec

IP Security Protocol

- It allows secure communication between IP-based services and applications.
- We must change the IPv4 stack to integrate
- It is incorporated IPv6 default.
- Benefits
  - Authentication / integrity
  - Confidentiality
  - Key management
  - Access control
  - Anti repetition
  - Compression

4.11. IPsec

IPSec is the standard for secure communication at level 3

- Developed by the security working group of the IETF IP
- Internet standard des 1998-99
- RFCs
  - RFC 2401, “Security Architecture for the Internet protocol”
  - RFC 2402, “IP Authentication Header”
  - RFC 2406, “IP Encapsulating Security Payload”
  - RFC 2407, “The Internet IP Security Domain of Interpretation for ISAKMP”

4.11. IPsec

Characteristics

- Transparent to applications
  - APIs TCP / UDP not changed
- Transparent to users
  - It is not necessary to have security knowledge
- IPSec can be implemented in a firewall or router
  - It ensures all traffic crossing the perimeter
  - No need to change the programs: the conversion is done by the firewall or router.
- *Applications*
  - *Virtual Private Networks* (VPN) on Internet
  - Secure remote access to Internet

4.11. IPsec

Characteristics

Applicable from:

- 2 hosts: security between machines
- 2 routers: protect a network link
- 1 host and a router: Secure Access

2 operating modes

- Transport: ditto IP but with security features
- Tunnel becomes an option for VPNs

It is flexible and extensible

- Not completely define the specifications of the algorithms to use
- It allows you to choose between different options and incorporate new

4.11. IPsec

Protocols used

Traffic safety protocols

- *Authentication Header* (AH)
  - It ensures integrity, authentication and duplicate detection
- *Encapsulating Security Payload* (ESP)
  - It provides confidentiality (encryption) and can authenticate

Key management protocols (IKE)

- *Internet Security Association and Key Management protocol* (*ISAKMP)*
  - To manage security associations
- *Oakley*
  - For the generation and management of keys

AH/ESP apply for each separate package.

Security Associations (SA)

- IPSec is based on the concept of Security Associations
  - Set all the information needed for secure communication between two devices
  - Are unidirectional relations between sender i receiver
  - For bidirectional communication takes two SAs
- Each SA is identified by:
  - *Security Parameter Index* (SPI)
    - Bit string it is acting as local Identifier
  - IP address of the recipient
  - Security Protocol Identifier (AH/ESP)

4.11. IPsec

Security Associations (SA)

- *Security Association Database* (SADB)
  - Database that contains the parameters of the SA.
  - Defines the parameters associated with each SA.
  - Every node has IPSec.
  - Different implementations are possible
- Operation
  - The transmitter:
    - When sending a package, see the SA in its SADB, processes and incorporates SPI
  - The receptor:
    - Analyzes the destination address and SPI, see the corresponding SA in its SADB and processes

4.11. IPsec

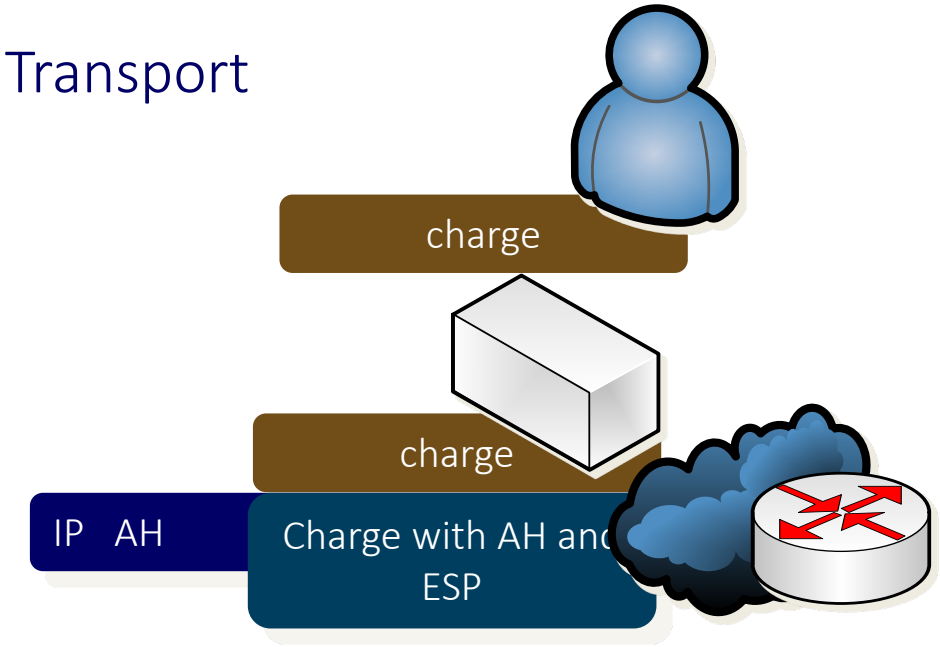
Parameters of them SA

- SA l*ife type* y *lifetime*
  - Type units (seconds or kilobytes) and TTL SA
- *Group description*
  - The Oakley group used in negotiating keys
- *Encapsulation mode*
  - Tunnel or transport
- *Authentication Algorithm*
- *Key Length and rounds*
- *ESP Information*
  - encryption algorithms, keys, key life time of ...
- *Sequence Number Counter*, Sequence Number Overflow, *Anti-Replay Window*
  - Anti-replay mechanisms

4.11. IPsec

Operating Modes

Transport



Tunnel

4.11. IPsec

Transport mode

It provides protection

- A protocol of the upper layer
  - That is, the charge packets IP
- All communication is secure (encrypted and / or authenticated)
  - Intermediate teams can not decrypt the packets

It is usually applied in end to end communications between end stations

Before IP header is added to the package, are added security

AH authenticates the charge IP and parts of the IP header

ESP encrypts and optionally authenticates the charge IP, the IP header is not protected

Tunnel mode

Protects the entire IP packet

It is usually applied in communications between gateways

- To protect datagrams generated or for non-IPSec (as with VPNs) systems.
- It applies when the IP header end to end is already attached to the package

Operation

- The headers AH / ESP are added to the IP packet
- The whole package is treated as if it were the charge of a new package with a new IP header

The packets travel through a tunnel

- Road routers are not able to examine the original package

4.12. Conclusions

Conclusions on IP and ICMP

IP Protocol

- Network layer protocol, routes and delivers information between machines of different networks.
- Unit info: IP datagram (one header and a data field).
- Connectionless and provides a best effort service, reliably provide higher levels.
- Use the subnet mask and routing tables for establishing routes.
- Due to the fragmentation and reassembly appears MTU
- ICMP protocol
- Part of IP that provides control functions, but does the most reliable IP protocol, only reports errors to the source machine.
- ICMP messages travel in the data field of the IP protocol, but not a high level protocol.

IPSec security protocol incorporating IP