# Computer Networks

## Lecture on

## ARP, IPv4, ICMP, DHCP, IPv6, NAT

## Plan of This Lecture

- ARP & RARP – Address Resolution Protocol & Reverse ARP
- IPv4
- ICMP – Internet Control Message Protocol
- DHCP – Dynamic Host Configuration Protocol
- IPv6
- ICMPv6
- NAT – Network Address Translation

# ARP & RARP – Address Resolution Protocol & Reverse ARP

ARP answers to:

„What is the physical address
of a station with a given network address?"

RARP answers to:

„What is the network address
of a station with a given physical address?"

The questions are broadcasted to the LAN segment

ARP

Who is asking?

- Every node sending a network packet

Who is answering?

- Owner of the network address – if exists in the LAN
- Router – if the address do not belong to the LAN

Answers are collected in the ARP table See it with: `arp -a`

RARP

Who is asking?

- Diskless station during a booting process: – What is my network address?

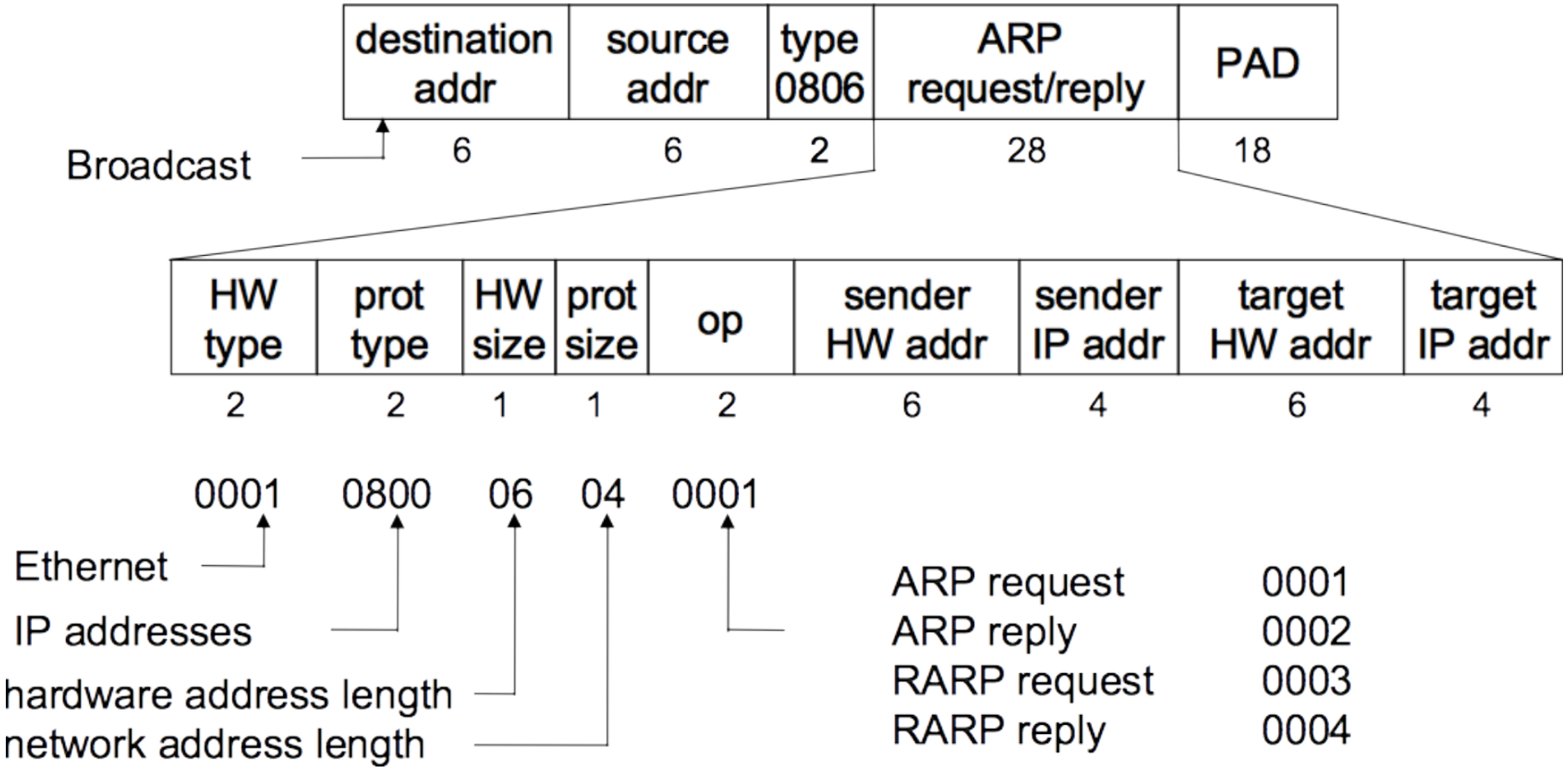
Who is answering?

- RARP server

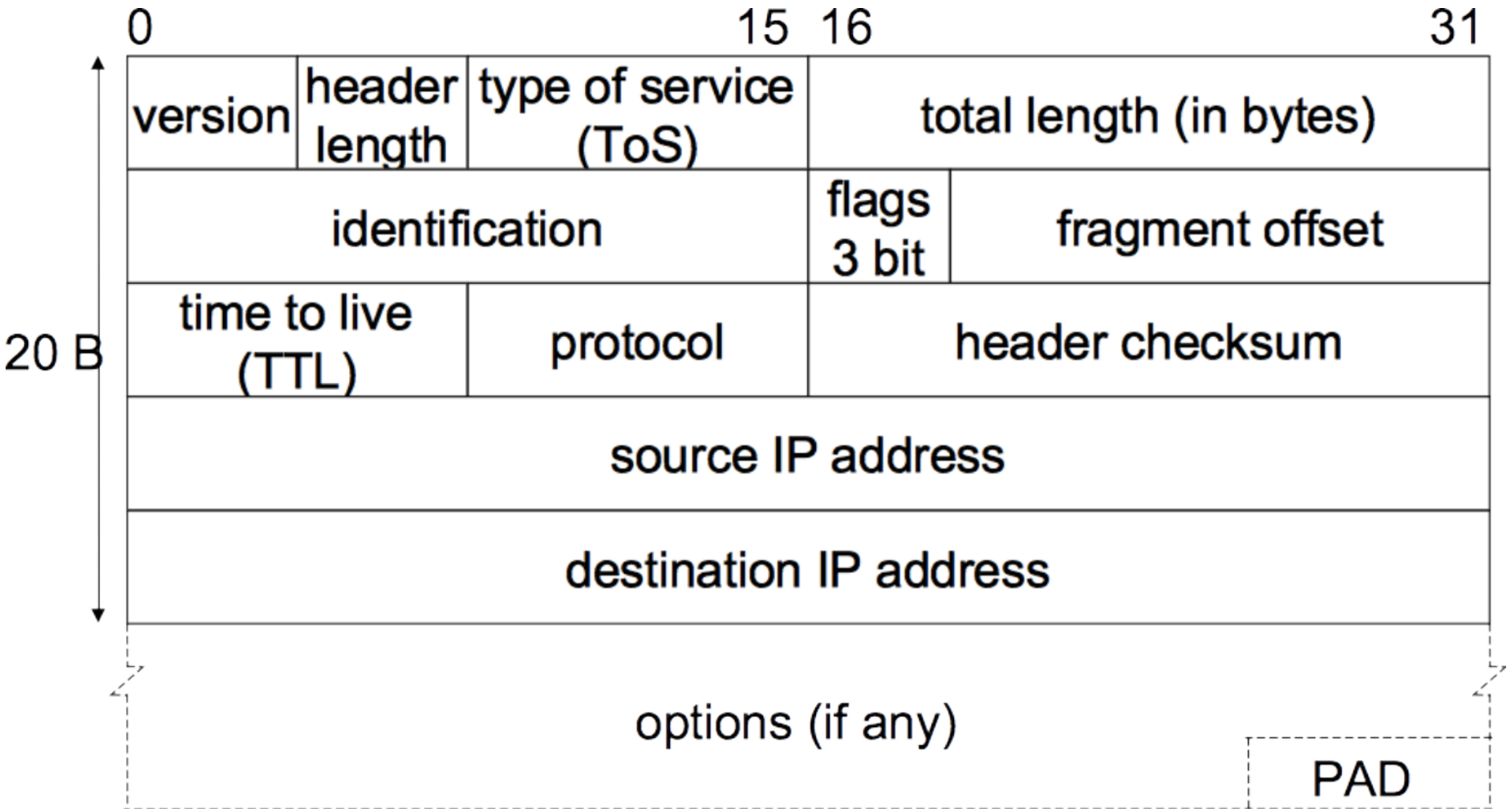
ARP & RARP were conceived for any kind of networks

They support any 2nd & 3rd layer protocols

*PAD is needed to get the minimum payload size of 46 octets*



# IPv4


0
15
16
31
version
header length
type of service (ToS)
total length (in bytes)
identification
flags 3 bit
fragment offset
time to live (TTL)
protocol
header checksum
source IP address
destination IP address
20 B
options (if any)
PAD

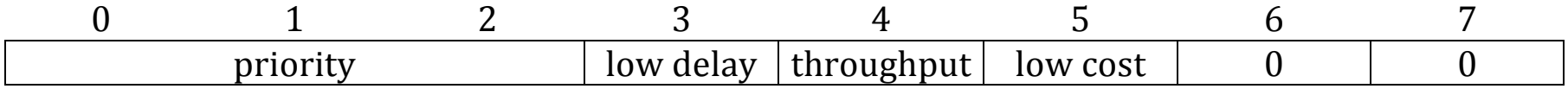
**Version** = 4

**Header length** = (5 + N) 32-bit words

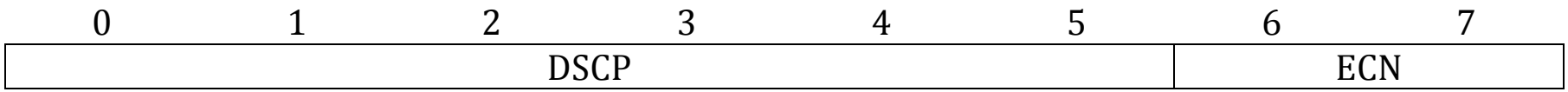
for this reason **PAD**ding can be needed

**ToS** – Type of Service

- originally defined as




- not used in most past networks
- in today's network it is replaced by




DSCP – Differentiated Services Code Point

specifies differentiated services (DiffServ)

– priorities assigned to well defined services

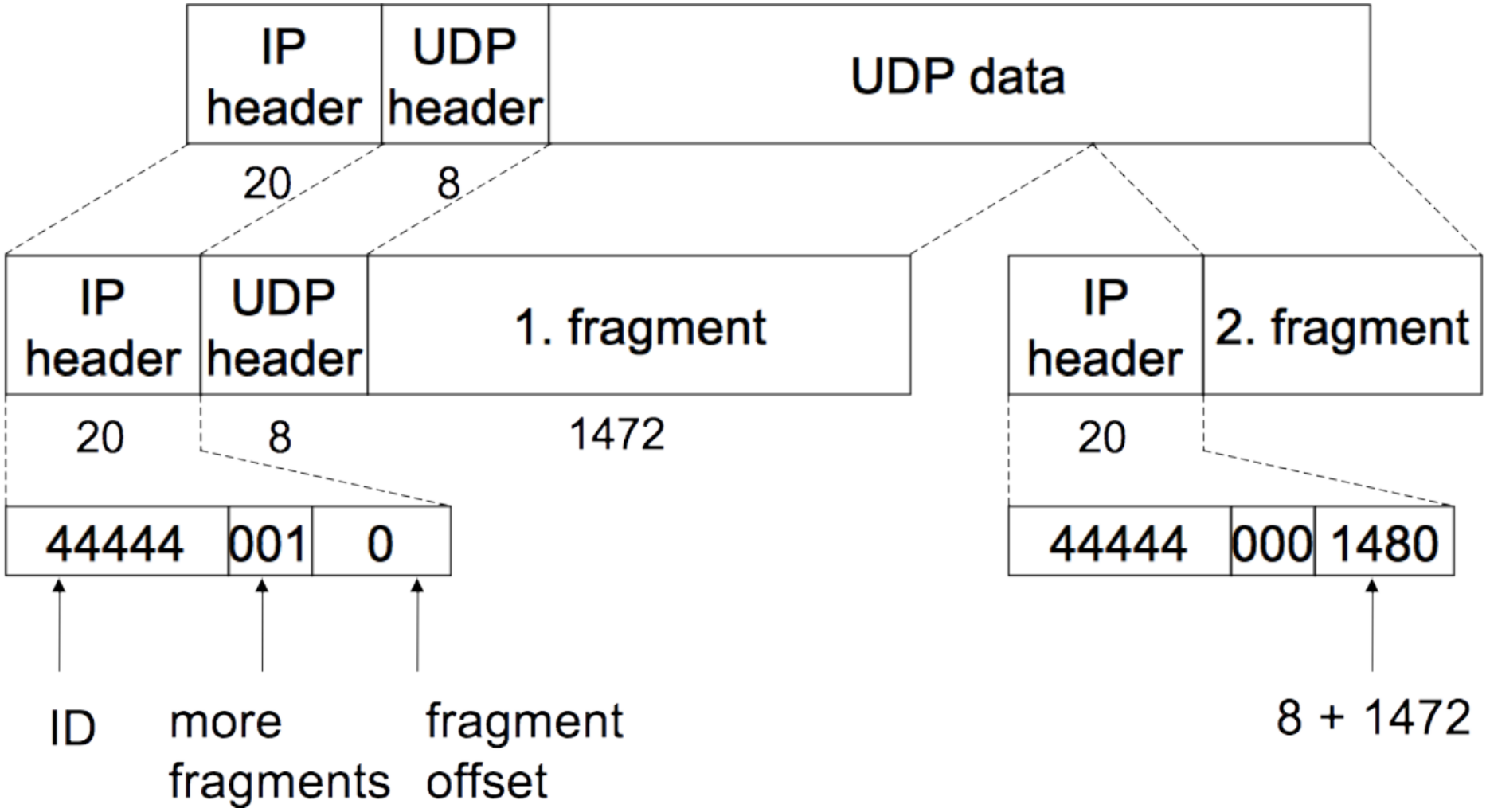
ENC – Explicit Congestion Notification

stamped by a congested router

**Flags**

- bit 0: Reserved; must be zero
- bit 1: Don't Fragment (DF)
- bit 2: More Fragments (MF)

# IP fragmentation



**Time-to-live**

nowadays it is number of hops

every router decrement it by 1

if =0 then packet is dropped

**Protocol**

defines payload – what is the next header

e.g.: 6 – TCP, 17 – UDP, 1 – ICMP

**Options**

- rarely used
- for control, testing, probing, experimentation
- some considered as unsecure & are blocked by some routers, e.g.:
  - loose source routing
  - strict source routing

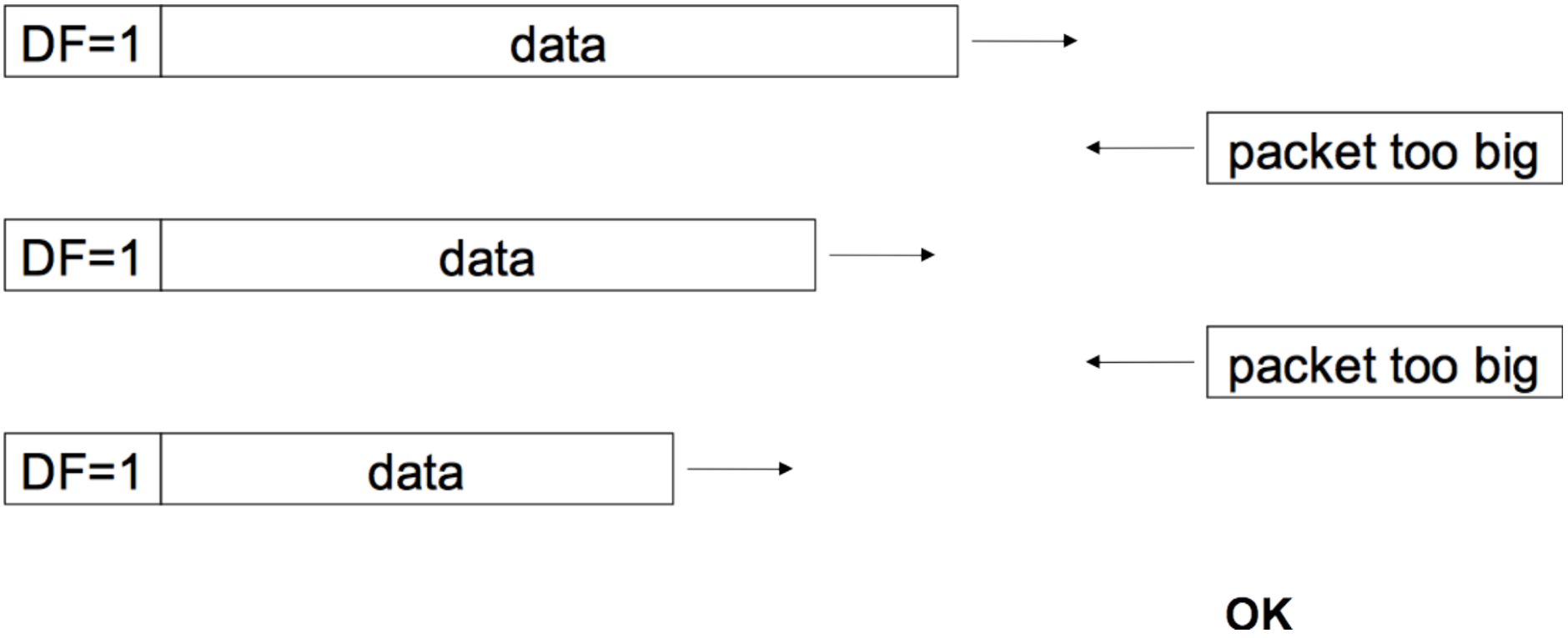
# ICMP – Internet Control Message Protocol

Aim: self-recovery from errors in the network

PDU types:

- echo request, echo response  Try: `ping host`  host – IP addr. or domain name
- destination unreachable
- packet too big
- stop packet source
- need to change the route
- TTL expired
- error in the IP header
- timestamp request, timestamp response
- subnet mask request, subnet mask response
- router solicitation, router advertisement
- …

# Path MTU Discovery



# DHCP – Dynamic Host Configuration Protocol

Aim: to assign an IP address and other network configuration parameters to each device in the LAN

**DHCP server delivers**:

- IP address & mask – for the asking interface
- Other addresses
  - default router
  - DNS servers
  - time servers
  - WINS servers
  - ...
- Other parameters
  - Domain name
  - Host name
  - File server & path to the operating system for booting
  - ...

**Examples of DHCP clients**

- workstations
- lightweight WiFi access points
- IP phones
- ...

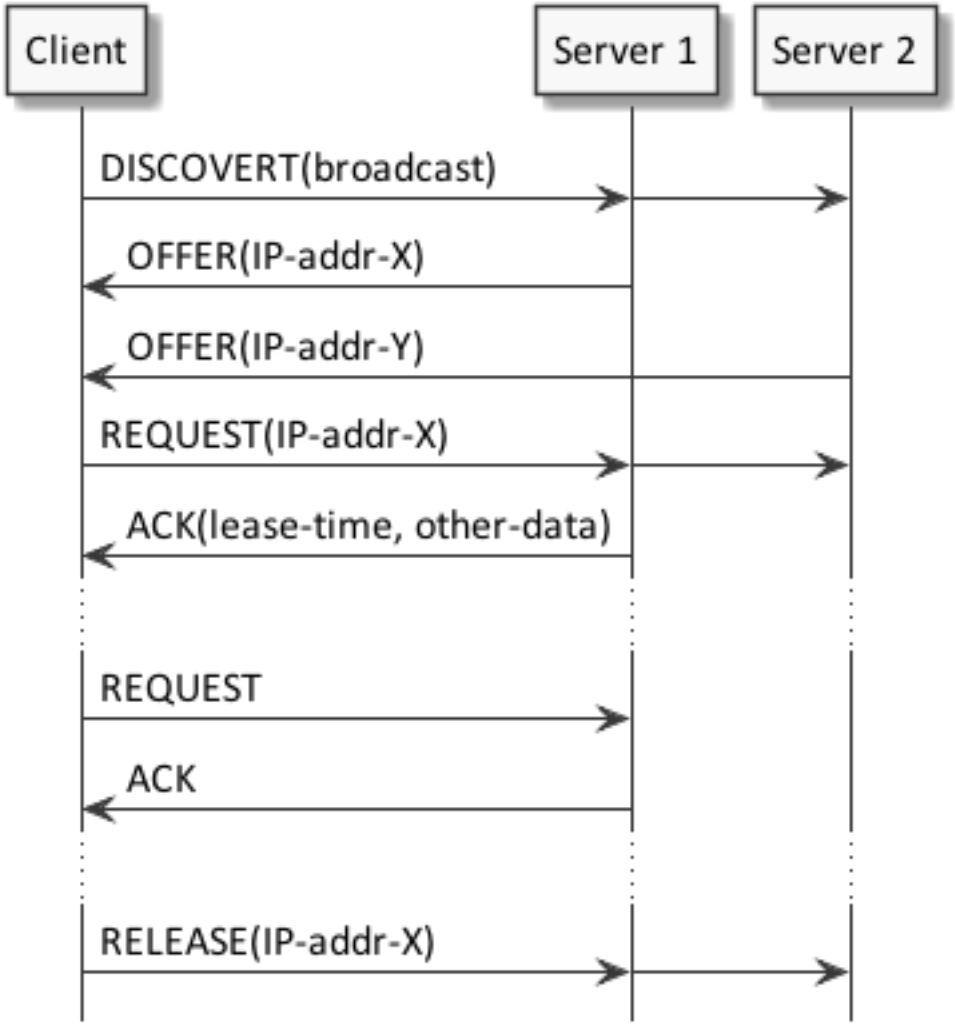
*DHCP works over UDP*

**Address allocation methods**

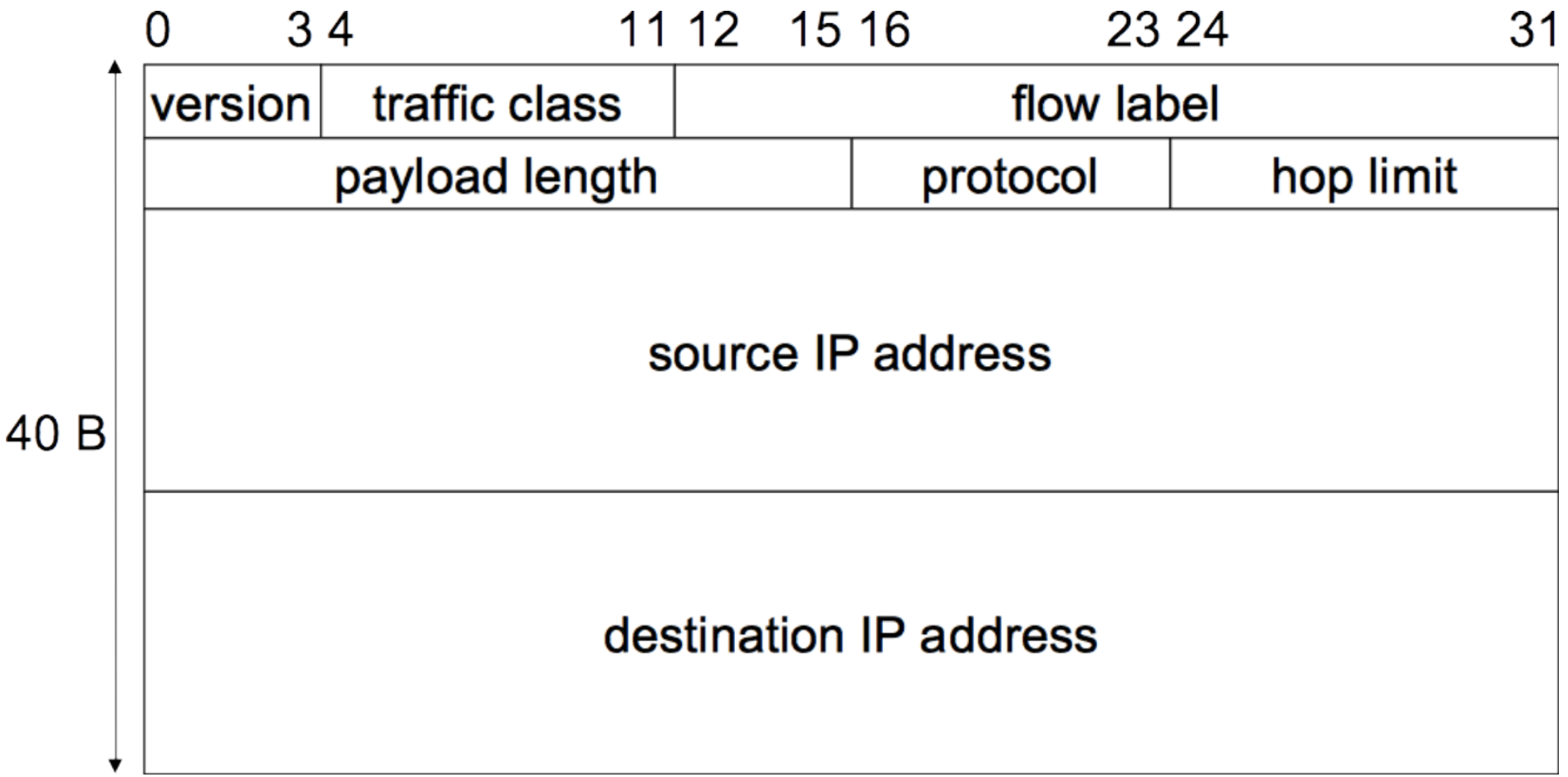
- Manually
  - MAC addr. to IP addr. mapping
- Automatically – permanently — e.g. for servers
  - from a given address range, set by an admin
- Dynamically – for a finite time (lease period) — e.g. for workstations
  - from a given address range, set by an admin
  - client may also request its last known IP address

**After the lease period**

- The address can be returned to the free addresses pool
  and allocated to the other client
- The client can also “refresh” the lease and retain the allocated address
- The client can be suspend from the network — e.g. after the end of a laboratory class


Client
Server 1
Server 2
DISCOVERT(broadcast)
OFFER(IP-addr-X)
OFFER(IP-addr-Y)
REQUEST(IP-addr-X)
ACK(lease-time, other-data)
REQUEST
ACK
RELEASE(IP-addr-X)

# IPv6


0
3 4
11 12
15 16
23 24
31
version
traffic class
flow label
payload length
protocol
hop limit
source IP address
destination IP address
40 B

**Version** = 6

Header length is constant = 40 B

**Traffic class**

- 6 bits – Differentiated Services (DS) field
  - well defined priorities for known services
- 2 bits – Explicit Congestion Notification

**Flow label** – with src. addr. allow to recognize packet flows

- Routers can use it
  - to speed-up forwarding
  - to direct a flow via the same path

# Main Features

- Huge address space
  - Optimistically around 4,000 trillions of addresses per 1 $m^2$ of the earth (considering different types of allocations)
  - Most pessimistically, at least 1,564 addresses per 1 $m^2$ of the earth
- End-to-end connectivity without NATs
- Efficient autoconfiguration – ad hoc & mobile networks
- Routers work faster
  - 1st header is simple and has constant length
  - No checksums
  - Simple subnetwork address aggregation
  - Flow label enables efficient packet processing

- Jumbograms
  - Can be as large as 4 GiB
  - Since both TCP and UDP include fields limited to 16 bits

    transport-layer tweaks are needed – RFC 2675
- Simple multihoming – access to the Internet via several ISPs
- Built in mobility mechanisms
- Built in security (IPSec)
- Header chain concept allows for future evolution
- Mechanism to co-work with IPv4 networks and to evolutionary migration from IPv4 to IPv6

# IPv6 Addresses

Hierarchy of IPv6 addressing

| 64 | | | | | | 64 |
|---|---|---|---|---|---|---|
| # Regional Internet Registry | # ISP level 1 | # ISP level 2 | # ISP level N | # organization | # localization | # host |

- Address autoconfiguration
  - Important for mobility & ad hoc networking
  - Stateless (obtained IPv6 prefix, own EUI-64 address)
    LAN submask has constant length = 64 bits
  - Stateless (obtained IPv6 prefix, randomly generated address)
  - Stateful – address from DHCPv6

- No broadcast addresses e.g. ARP broadcast load is replaced by ICMPv6 multicast
- Anycast addresses
  - Used by routing protocols, network security systems, …
  - Selected from the unicast address space
  - Assigned to more than one interface
    Typically belonging to different nodes
  - Routed to the nearest interface having that address
    According to the routing protocols' measure of distance
- Addressing scopes

| **unicast** | **multicast** |
|---|---|
| loopback | interface-local |
| link-local | link-local |
| | realm-local |
| | admin-local |
| | site-local |
| unique-local | organization-local |
| global | global |

# IPv6 Header Extensions

IP options have been moved to a set of optional Extension Headers

Extension Headers are chained together and placed between IPv6 and transport layer headers

| IPv6 Header<br>Next = TCP H. | TCP Header | Application Data |
|---|---|---|

| IPv6 Header<br>Next = Routing H. | Routing Header<br>Next = TCP | TCP Header | Application Data |
|---|---|---|---|

| IPv6 Header<br>Next = Security H. | Security Header<br>Next = Fragmentation | Fragmentation Header<br>Next = TCP | TCP Header | Application Data |
|---|---|---|---|---|

# IPv4 to IPv6 Transition Mechanisms

- Dual stack – supports both IPv4 and IPv6
  - Modern OSs do it

- Stateless IP/ICMP Translation translates packet header formats IPv6 ↔ IPv4
  - Address prefix ::ffff:0:0:0/96 ::ffff:0:a.b.c.d ↔ a.b.c.d
  - IPv4 net can connect 2 IPv6 nets
  - IPv6-only hosts can communicate with IPv4-only hosts

- Tunnelling – encapsulating IPv6 packets within IPv4
  tunnel broker is a service which provides a network tunnel
  - encapsulated within IPv4 packets using protocol number 41
  - encapsulated within UDP packets e.g. in order to cross a router or NAT device
  - use generic encapsulation schemes, such as AYIYA or GRE
  - SATAP – treats the IPv4 network as a virtual IPv6 local link
  - **Teredo** – an automatic tunnelling technique that uses UDP encapsulation
    (is claimed to be able to cross multiple NAT boxes)
  - **6in4** – configured tunnelling – used by enterprises

- Proxying and translation
  - dual-stack application-layer proxy
  - **464XLAT** allows clients on IPv6-only networks to access IPv4-only Internet services
    e.g. Skype
  - …

# ICMPv6

Supports IPv6 addresses

Covers functionalities of diverse IPv4 related protocols and adds more, e.g.:

- ICMP
- ARP & RARP – here is called Neighbour Discovery Protocol
- Internet Group Management Protocol – here is called Multicast Listener Discovery
- Multicast Router Discovery
- …

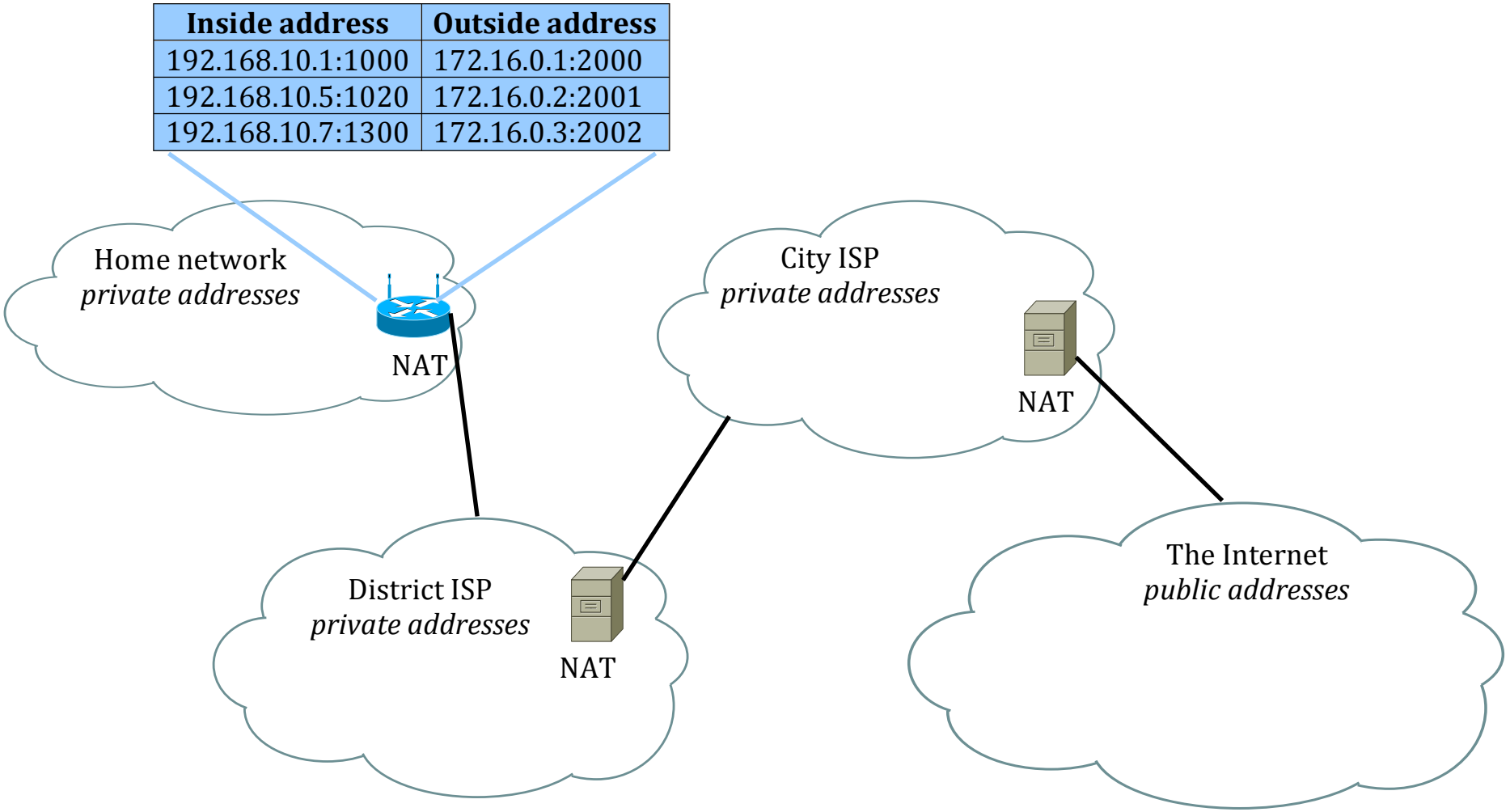
Try: `ping6 host`

## NAT – Network Address Translation

- Conceived as a short term solution for IPv4 address shortage
- Enables hosts an a private network to communicate with hosts on the Internet
- IP addresses and possibly port numbers

  are replaced at the boundary of a private network
- NAT server has address translation table
- Often installed on routers

## Example Chain of NAT Servers



# NAT Problems

- Outside IP address pool is smaller than inside pool
- How long to keep a translation record?
  - Many protocols are connectionless
- How to deal with
  - protocols that do not carry a port number, e.g. ICMP?
  - protocols that carry embedded IP addresses or port numbers?
    - e.g. in order to redirect responses or queries
  - IP multicast?

# NAT Advantages

- Public addressing space savings
- Elimination of need for LAN(s) readdressing when changing an ISP
- Elimination of need for ISP access readdressing when changing an ISP
- Local network security improvement is illusory
  even thought stated in many publications
  - Many attacks starts from internal network, from infected computers
  - Internal host which started communication with an outside one is visible from outside
    and can be attacked from outside
    - If it is not TCP communication, then if it ends, then the host is still visible until timeout
      – can be a few seconds

# NAT Disadvantages

- Main Internet concept is broken – the same visibility of every communication point
  - difficulties for applications demanding full network visibility
    (e.g., IP telephony, network games) – mitting point or proxy servers are needed
  - difficulties with server placing behind NATs – dynamic DNS services are needed
  - difficulties with sensor networks placement
- NAT server is a bottleneck for network throughput
  - have to keep state of every connection
  - cannot support many servers on local side
    - many users want to expose theirs HTTP servers
  - implementation in hardware is impossible
- Battery save terminals (e.g., portable phones) cannot be placed behind a NAT
- Disable integrity verification of IP headers (IPSec)
- Application that use several ports usually needs a proxy installed on NAT server (e.g., FTP)
- Integration of two networks, which use the same private address space, is difficult

# Summary

- ARP & RARP – Address Resolution Protocol & Reverse ARP
- IPv4
  - IP fragmentation
- ICMP – Internet Control Message Protocol
  - Path MTU discovery
- DHCP – Dynamic Host Configuration Protocol
- IPv6
  - Main features
  - Addressing
  - Header Extensions
  - IPv4 to IPv6 transition/coexistence mechanisms
- ICMPv6
- NAT – Network Address Translation
  - Problems
  - Advantages
  - Disadvantages

# Exercises

Run in a terminal window the following commands and figure out the output

```
arp -a
ping -c3 www.qzhu.edu.cn
ping6 -c3 en.wikipedia.org
traceroute www.ii.pw.edu.pl
```

Take a look into `man tcpdump`

To do the following exercises, you need to have the root permissions

| 1st terminal window | 2nd terminal window |
|---|---|
| Run<br>`sudo tcpdump -vl icmp`<br>Observe and explain the output<br>Stop it by pressing Ctrl-C | Run<br>`ping -c1 www.qzhu.edu.cn` |
| Run<br>`sudo tcpdump -vl icmp6`<br>Observe and explain the output<br>Stop it by pressing Ctrl-C | Run<br>`ping6 -c1 en.wikipedia.org` |

# Questions

1. What for a host uses ARP and RARP (Reverse Address Resolution Protocol)?
2. How does ARP (Address Resolution Protocol) work?
3. What for is the hop count field in the IP header?
4. What for is the protocol field in the IP header?
5. What for is the Type of Service / Traffic Class field in the IP header?
6. What is the aim of the Time to Live field in IPv4 header (hope limit in IPv6)?
7. What is the aim of ICMP?
8. What for a host uses DHCP (Dynamic Host Configuration Protocol)?
9. How many DHCP servers can work in a network segment?
10. What are main advantages of IPv6?
11. What is it anycast address, and for what is it used (example of applications)?
12. What are the purposes of local-link and unique local IPv6 addresses?
13. Mention principal transition mechanism to use IPv6 in IPv4 world.
14. What is the IPv6 tunnel broker service?
15. How an IPv4 address is mapped into IPv6?
16. What is the difference between ICMPv4 and ICMPv6?
17. Why is better to process fragmentation/defragmentation on terminal devices than on routers?
18. What was the reason for introduction of NAT (Network Address Translation) into Internet?
19. What are main disadvantages of NAT?