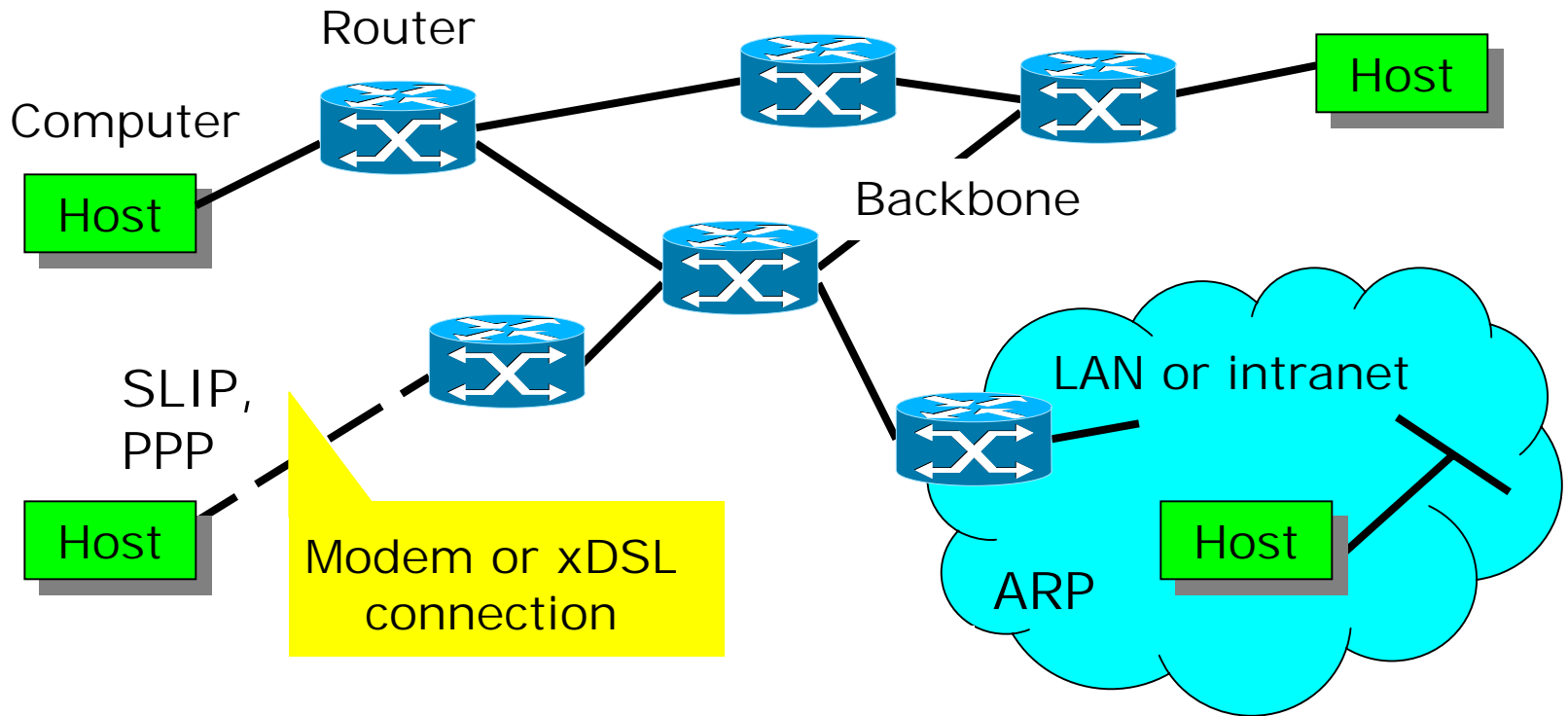


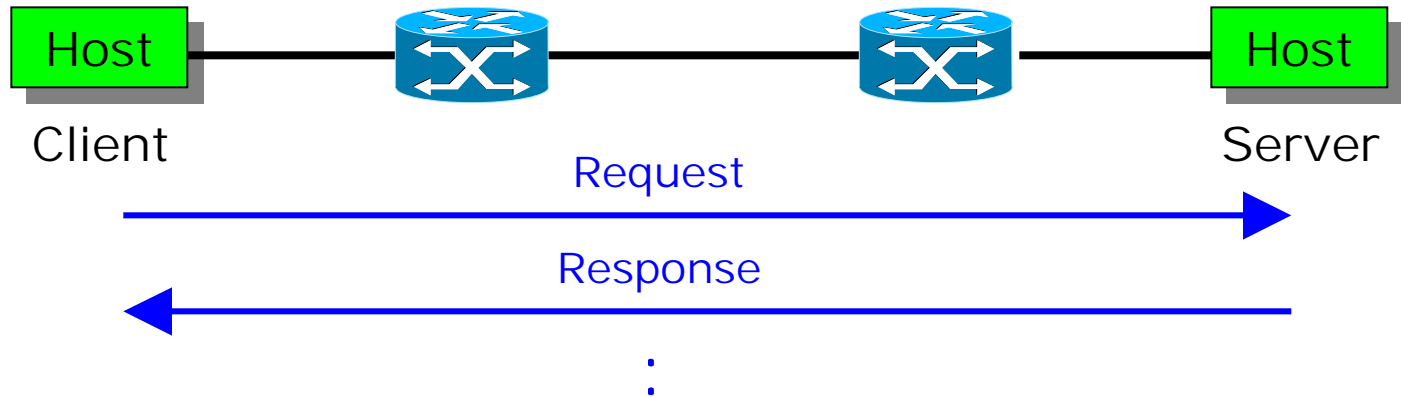
# Internet, Part 1

- 1) Internet basic concepts
- 2) The IP protocol stack
- 3) The IP datagram header (IPv4 and IPv6)
- 4) Addressing and routing
- 5) Example: downloading HTML page
- 5) Why IPv6?

# IP network architecture

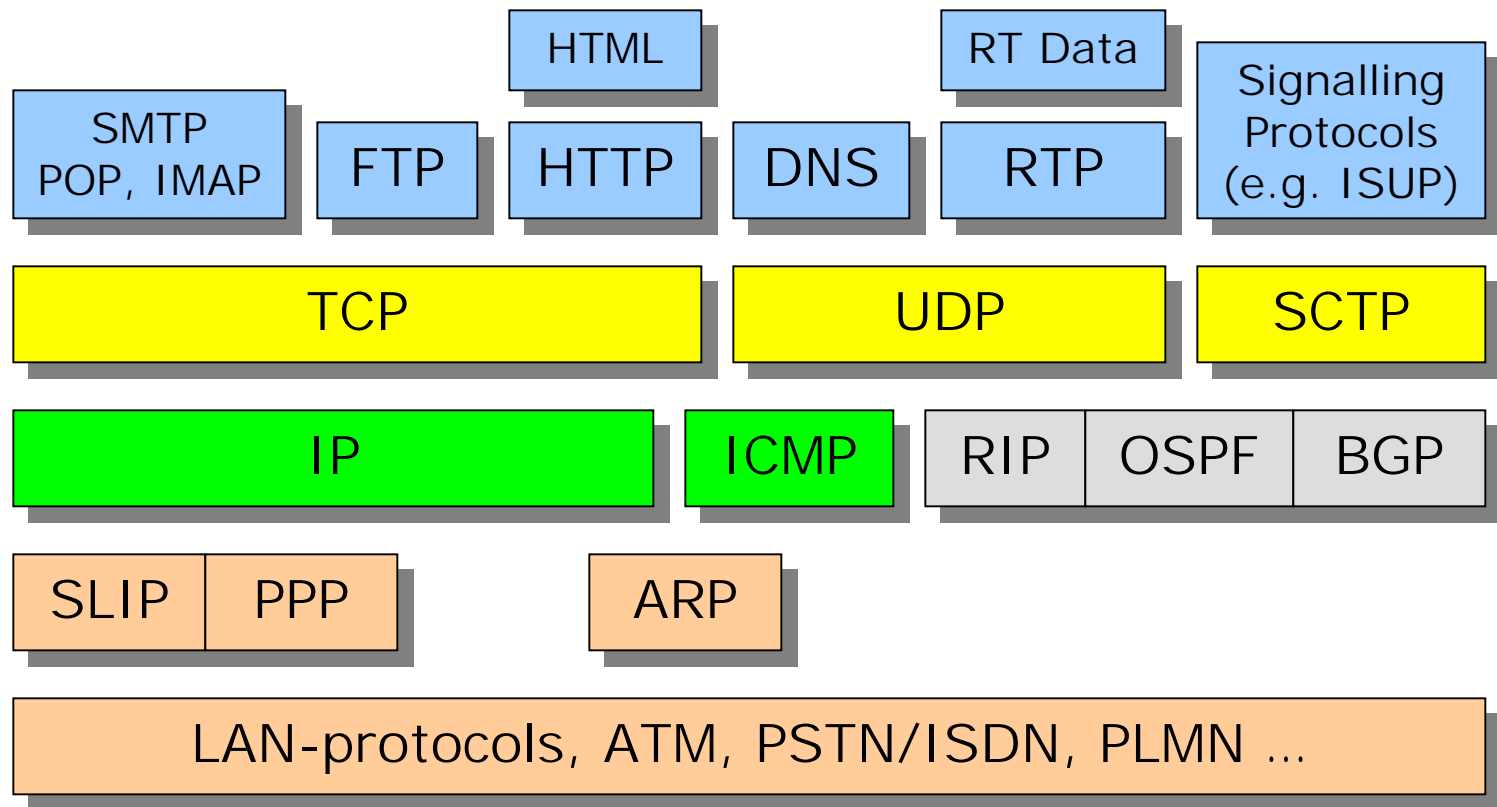


# Client-server concept

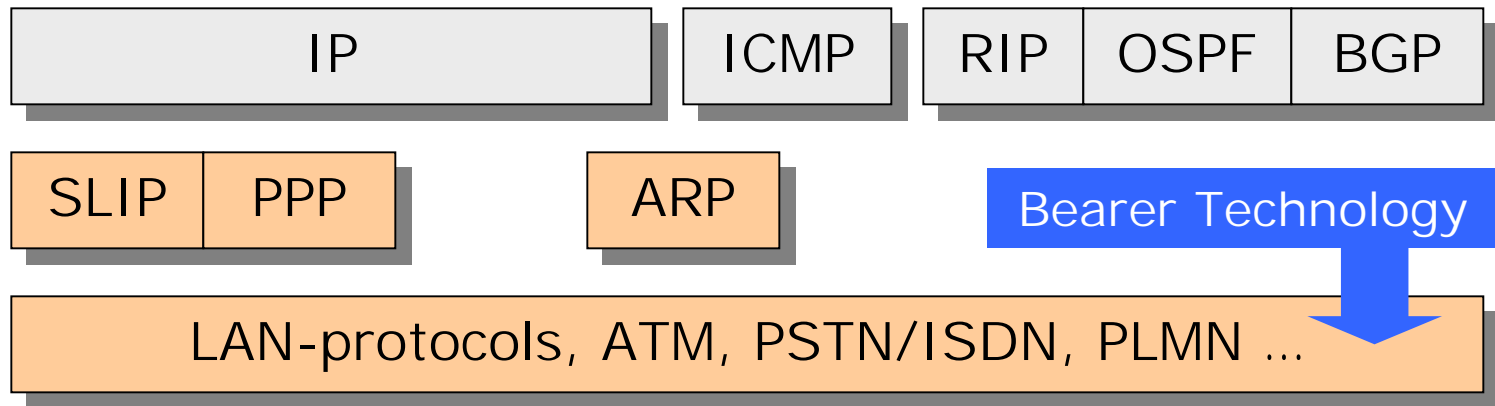


- Transactions are always started by client
- Network does not have to know IP address of client before transaction
- Clients can be behind dial-up modem connections
- Web (www) applications are based on this concept

# IP protocol suite



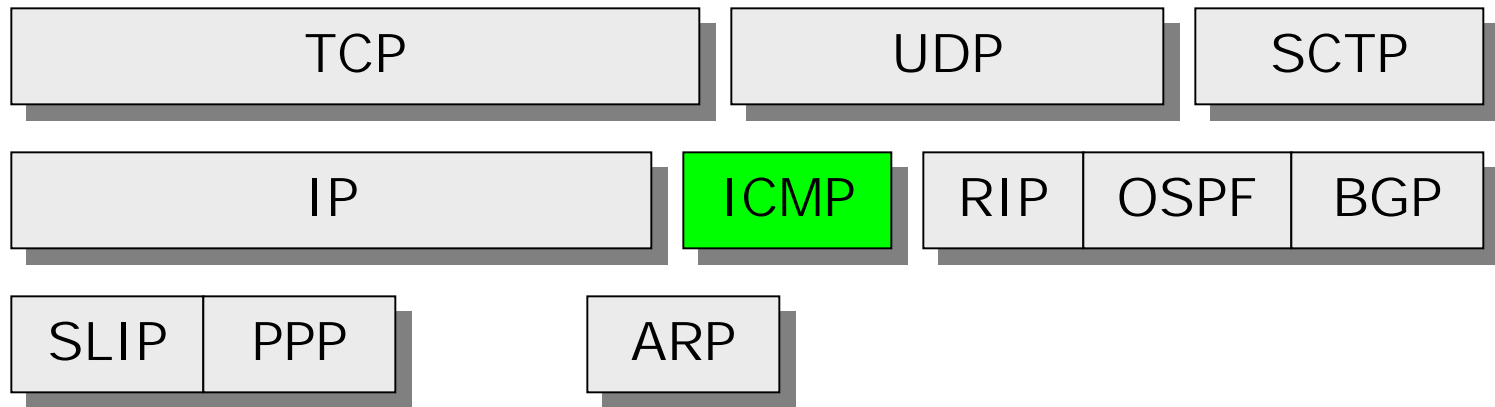
# Lower protocol layers



ARP (Address Resolution Protocol) takes care of mapping between logical IP addresses and physical MAC addresses in a Local Area Network (LAN).

PPP (Point-to-Point Protocol) or SLIP (Serial Line IP) is used for transport of IP traffic for instance over modem connections (between terminal and ISP's PoP).

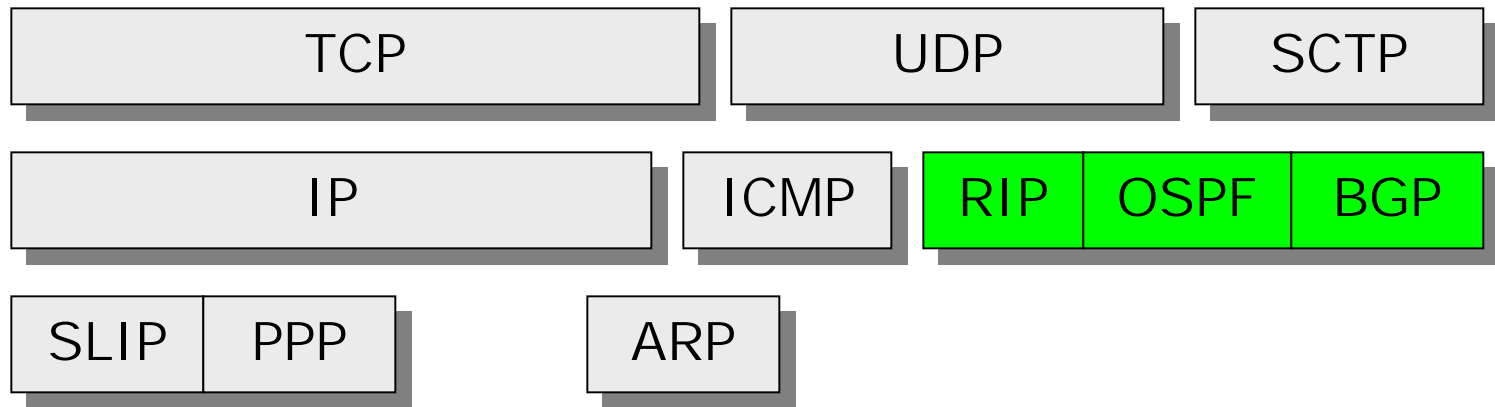
# Assisting protocols at the IP layer (1)



ICMP (Internet Control Message Protocol) is a mandatory protocol (i.e. must be supported by all routers) used for informing hosts about problems in the network.

**Some ICMP messages:** Destination network/host/port unreachable/unknown, echo request, echo reply, TTL expired, IP header bad.

## Assisting protocols at the IP layer (2)



Various routing protocols are employed for exchanging information between routers in the IP network

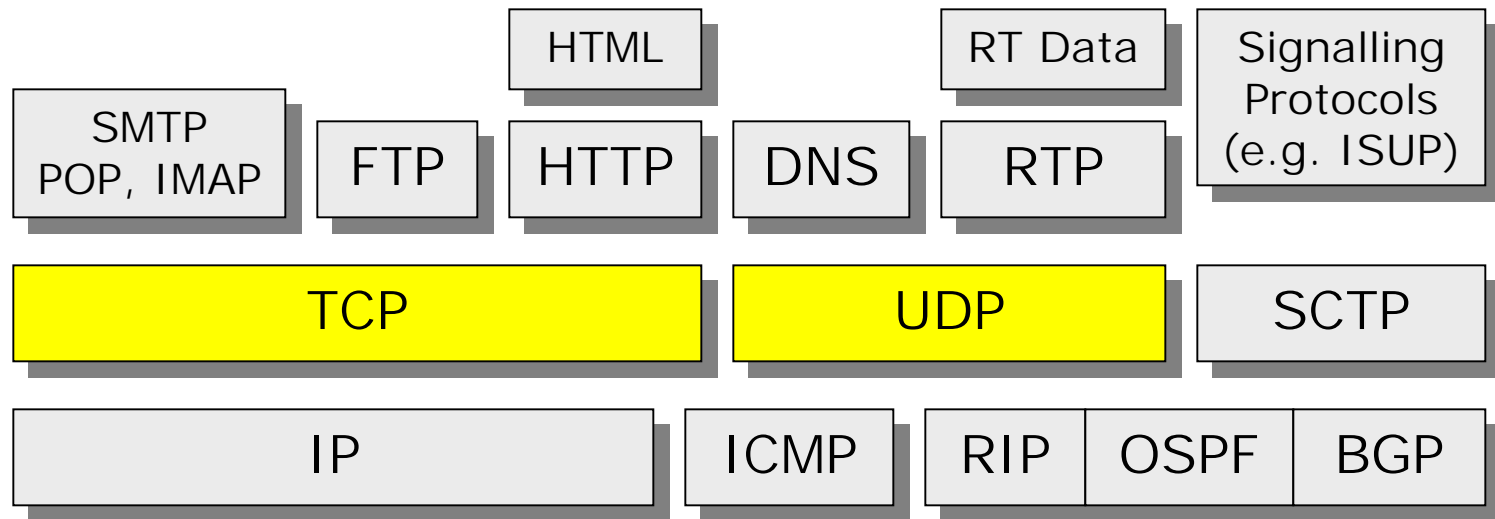
RIP (Routing Information Protocol)  
OSPF (Open Shortest Path First)

for routing within  
autonomous systems

BGP (Border Gateway Protocol)

for "international" routing

# Transport layer protocols (1)

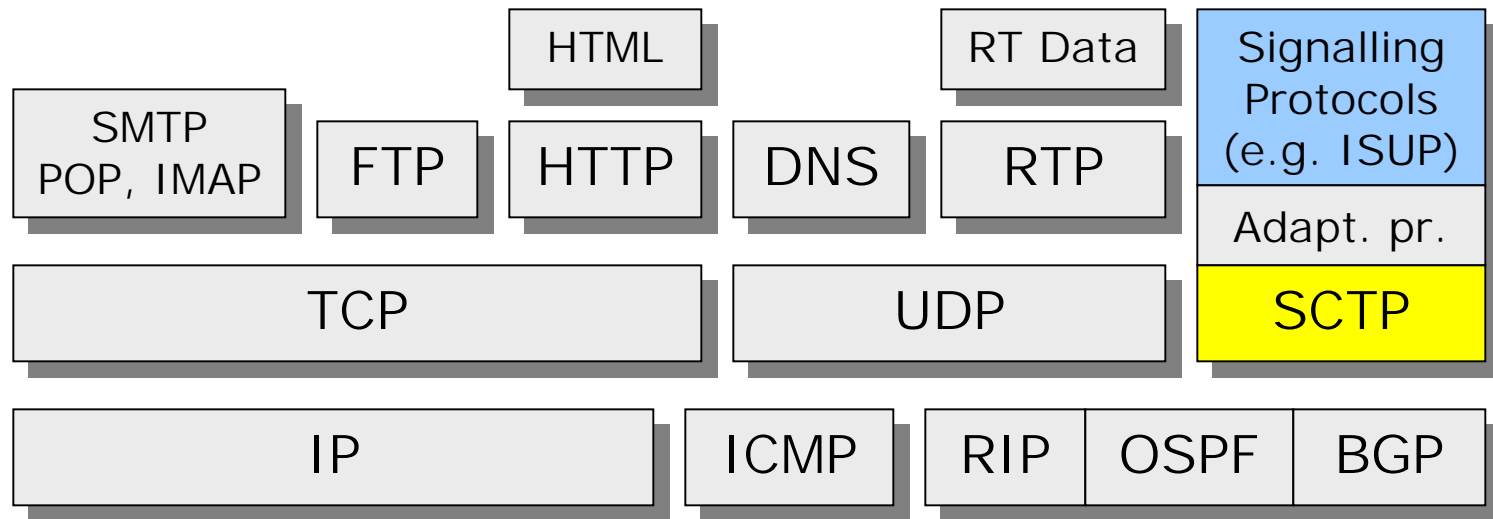


TCP (Transmission Control Protocol) takes care of end-to-end flow & error control + segmentation & reassembly of larger blocks of information.

UDP (User Datagram Protocol) is used for "unreliable but fast" transport of smaller blocks of information.

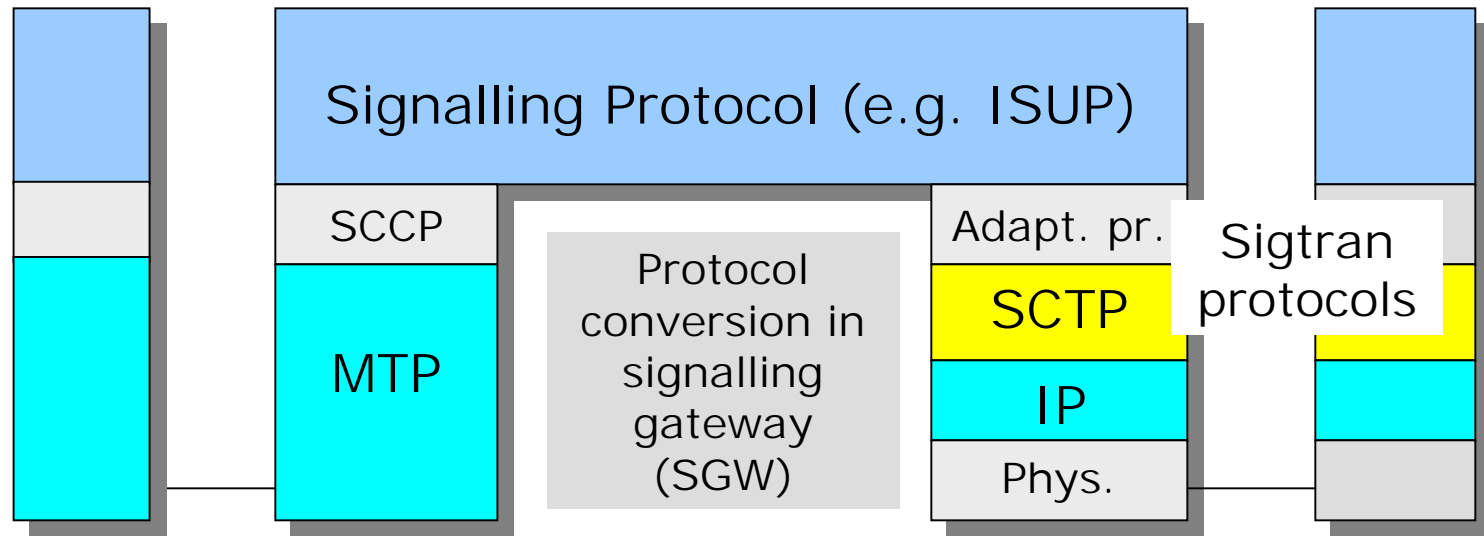


## Transport layer protocols (2)



SCTP (Stream Control Transmission Protocol) is an alternative to TCP (= > **too slow**) or UDP (= > **not reliable enough**) for carrying signalling information (ISUP, MAP, RANAP ...) over IP networks.

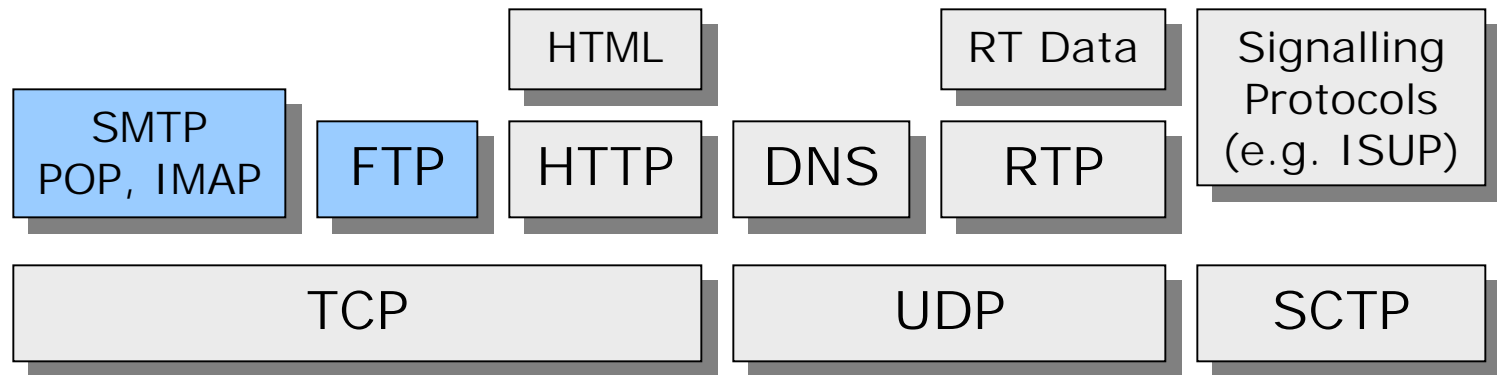
# SCTP is used for signalling transport



Transport of SS7 type application protocols (e.g. ISUP) in SS7 network using **MTP** (+ SCCP)

Transport of SS7 type application protocols (e.g. ISUP) over IP network using **Sigtran** protocols

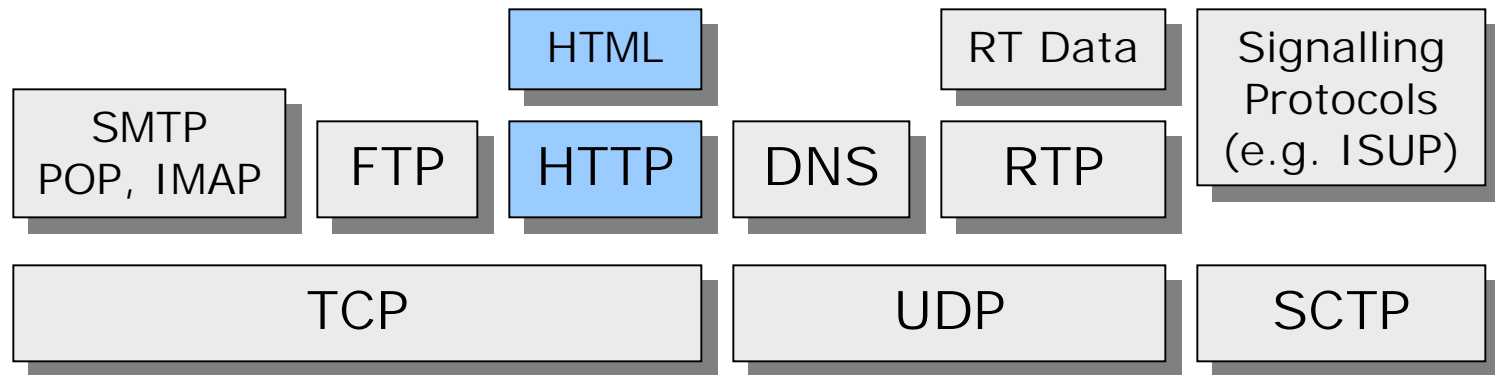
# Applications (1)



FTP (File Transfer Protocol) for sending larger files (offers flow and error control).

SMTP (Simple Mail Transfer Protocol) for **outgoing e-mail**.  
POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) for **fetching e-mail from mailbox**.

## Applications (2)



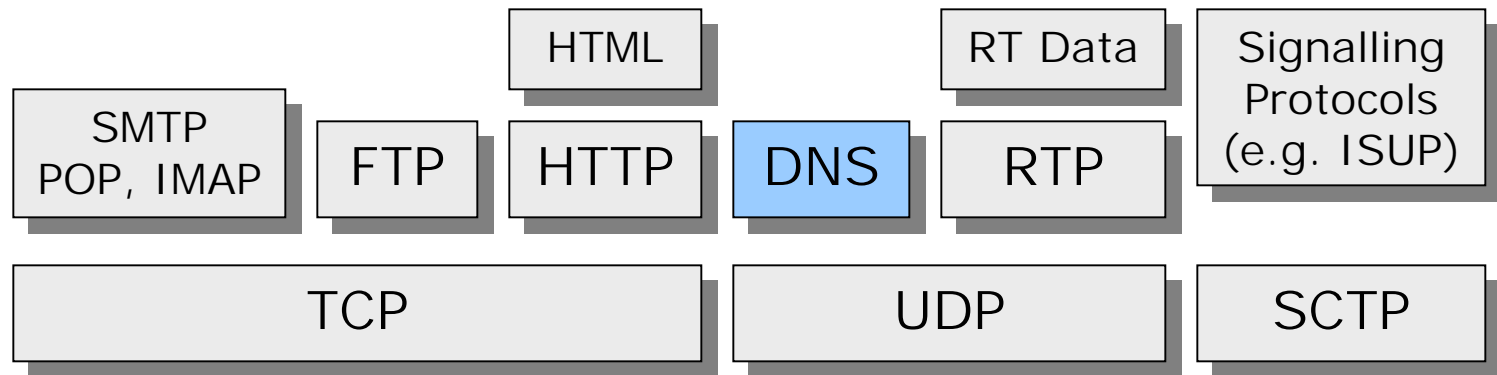
HTTP (HyperText Transfer Protocol) is used for client-server type of communication, and is the most popular protocol for transport of Web content (e.g. HTML pages).

<http://www.hut.fi/overview.html> ← Uniform Resource Locator (URL)

↑                    ↑                    ↑

protocol    host computer    content page written in HTML

# Applications (3)



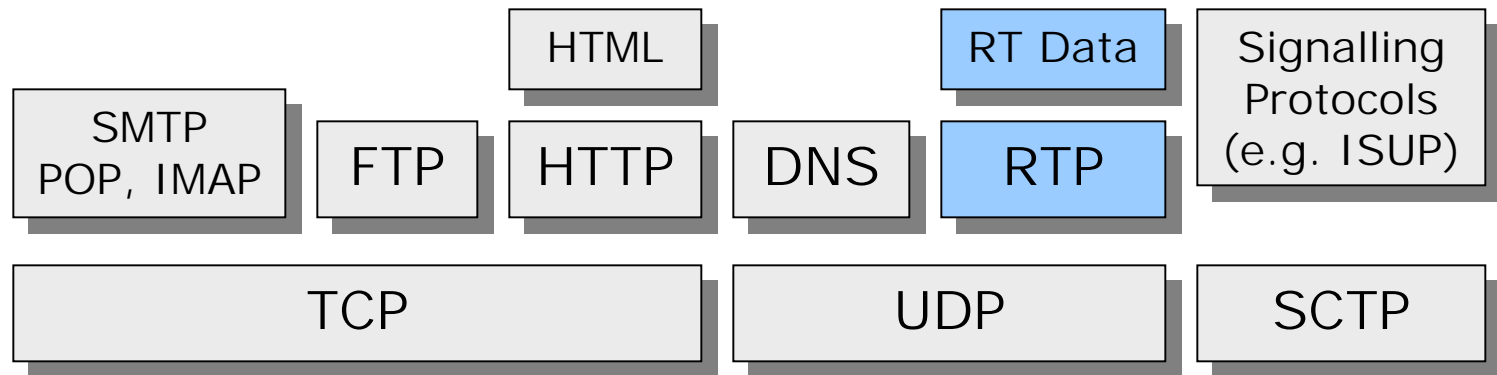
DNS (Domain Name System) performs translation between IP addresses and domain names:

122.233.121.123 ↔ thisnetwork.thishost.com

IP address must be used for routing through IP networks

However, domain names are more user friendly

# Applications (4)

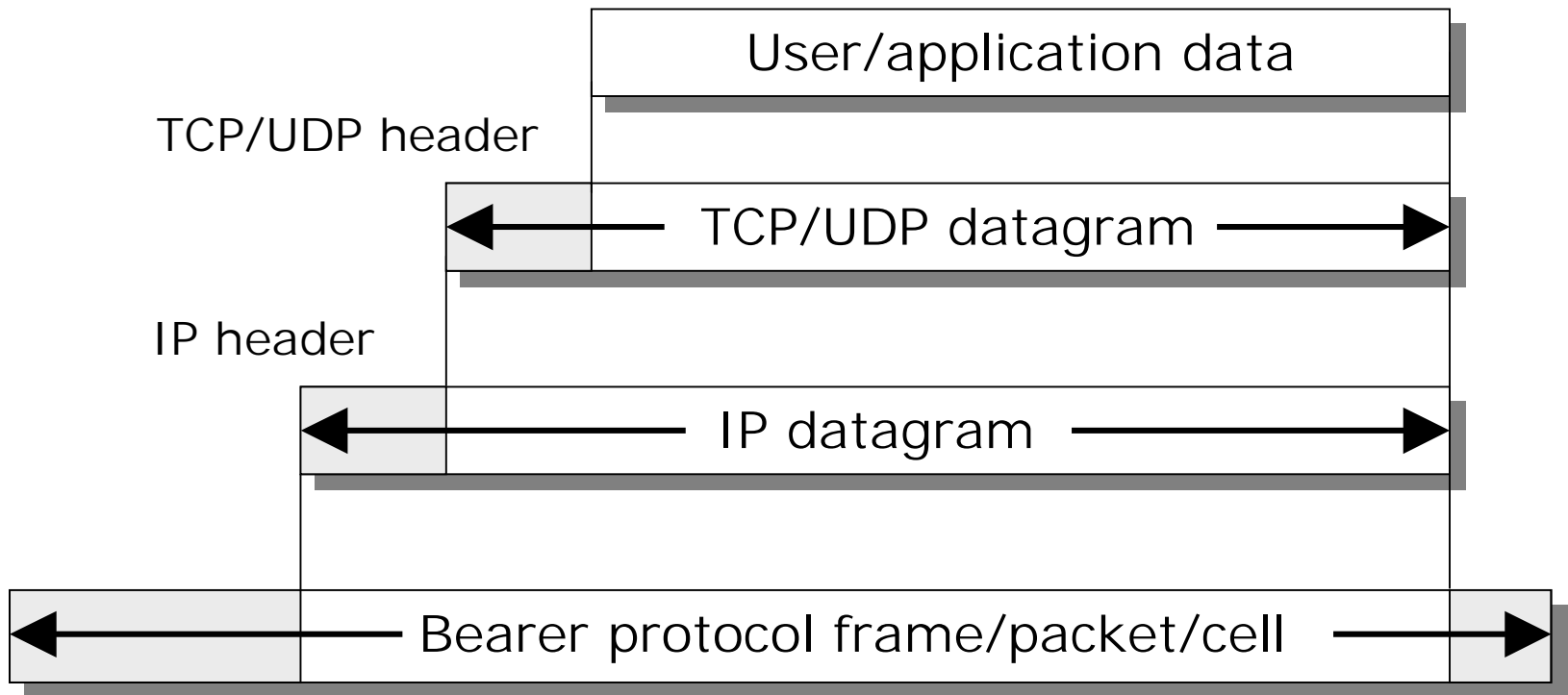


RTP (Real Time Protocol) provides important functions (e.g. sequence numbering, time stamp) for transport of **real time data**. RTP typically runs on top of UDP.

RTP can carry e.g.

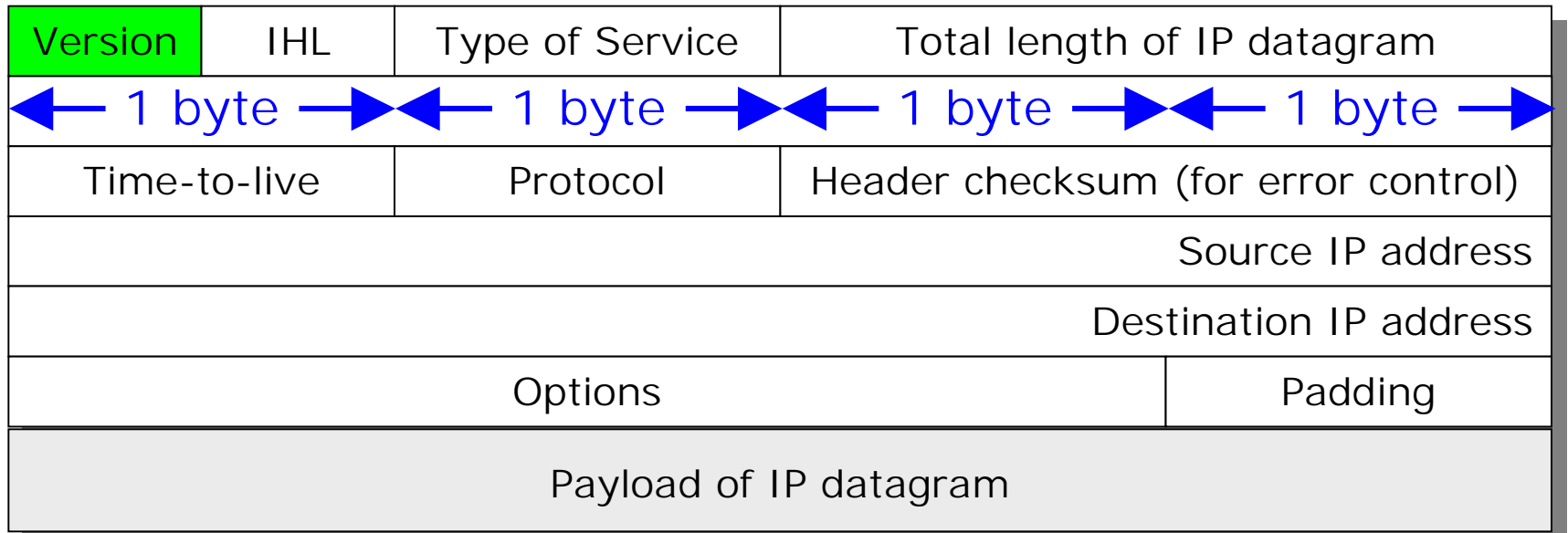
- PCM signals
- encoded speech (EFR, AMR)
- multimedia traffic  
(compressed audio, video)

# Typical IP packet structure



← Direction of transmission

# IPv4 header structure (1)



**Version** (4 bits): tells that this is IP Version 4 (IPv4)

(In case of IPv6, the following bits should be interpreted totally differently)



## IPv4 header structure (2)

Version	IHL	Type of Service	Total length of IP datagram	
Identification		Flags	Fragment offset	
Time-to-live	Protocol		Header checksum (for error control)	
Source IP address				
Destination IP address				
Options			Padding	
Payload of IP datagram				

Header length (4 bits) is needed since Options + Padding can vary in length.

(The Options field is rarely used. This is why such a field is not included in the IPv6 header)

## IPv4 header structure (3)

Version	IHL	Type of Service	Total length of IP datagram	
Identification			Flags	Fragment offset
Time-to-live	Protocol		Header checksum (for error control)	
Source IP address				
Destination IP address				
Options				Padding
Payload of IP datagram				

**ToS = Type of Service** (8 bits) is used for QoS management purposes (=> DiffServ).

(In the IPv6 header there is an 8 bit **Traffic class** field for the same purpose)

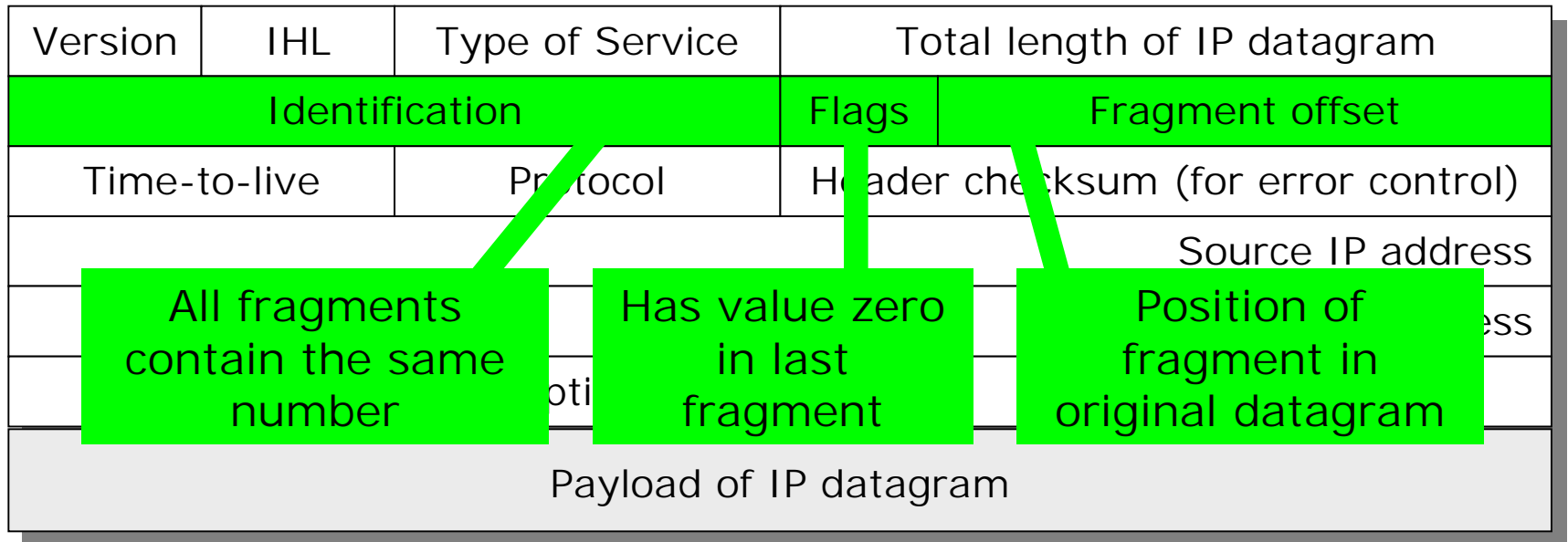
## IPv4 header structure (4)

Version	IHL	Type of Service	Total length of IP datagram	
Identification			Flags	Fragment offset
Time-to-live	Protocol		Header checksum (for error control)	
Source IP address				
Destination IP address				
Options				Padding
Payload of IP datagram				

**Datagram length** (16 bits): since this field is 16 bits long, the IP datagram can contain up to  $2^{16} = 65535$  bytes (in theory).

Most routers, however, cannot handle such large datagrams.

## IPv4 header structure (5)

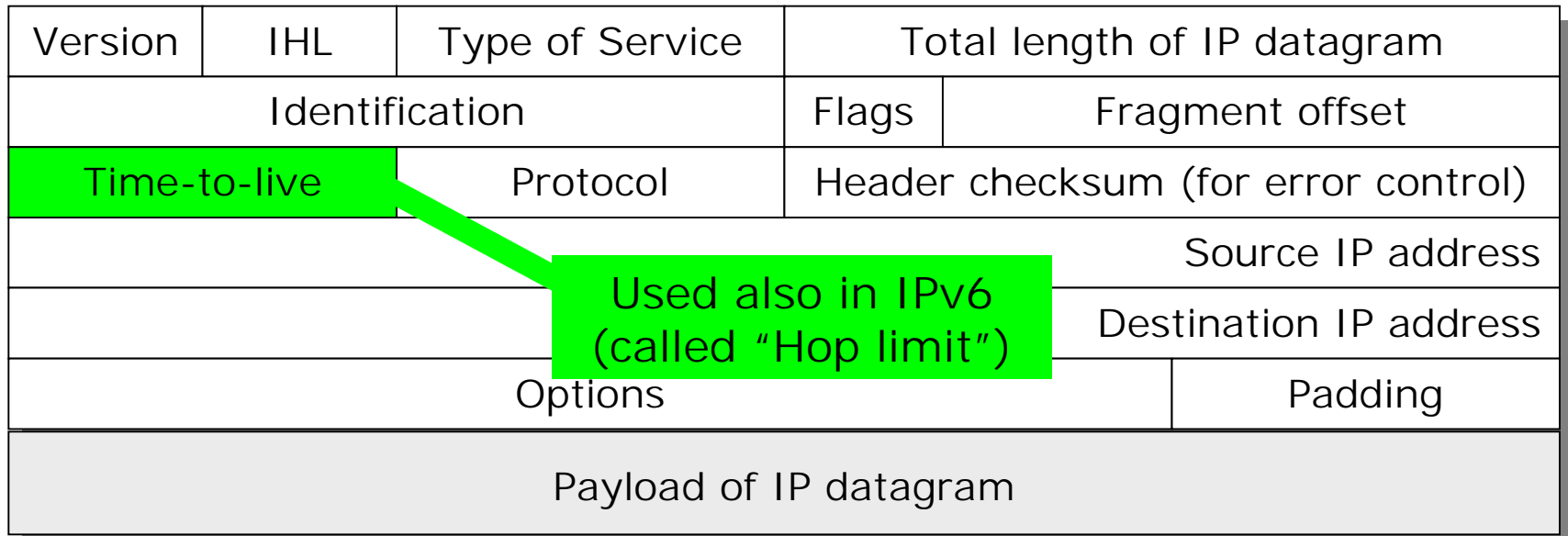


**IP fragmentation:** a large IP datagram may be fragmented (in any router along the path) and will be reassembled at the destination.

IPv6 does not offer fragmentation (it is rarely used anyway).

## IPv4 header structure (6)

Version	IHL	Type of Service	Total length of IP datagram	
Identification			Flags	Fragment offset
Time-to-live	Protocol		Header checksum (for error control)	
				Source IP address
				Destination IP address
Options			Padding	
Payload of IP datagram				



The diagram shows the IPv4 header structure as a table with five columns and seven rows. The first row contains 'Version', 'IHL', 'Type of Service', and 'Total length of IP datagram'. The second row contains 'Identification', 'Flags', and 'Fragment offset'. The third row contains 'Time-to-live', 'Protocol', and 'Header checksum (for error control)'. The fourth row contains 'Source IP address'. The fifth row contains 'Destination IP address'. The sixth row contains 'Options' and 'Padding'. The seventh row contains 'Payload of IP datagram'. A green callout box with the text 'Used also in IPv6 (called "Hop limit")' points to the 'Time-to-live' field in the third row.

**Time-to-live** (8 bits): this number is decreased by one in each router along the path. If number zero is reached in a router, IP datagram is discarded and router sends an ICMP message (TTL expired) to the source of the datagram.

## IPv4 header structure (7)

Version	IHL	Type of Service	Total length of IP datagram	
Identification			Flags	Fragment offset
Time-to-live	Protocol		Header checksum (for error control)	
			Source IP address	
			Destination IP address	
Options			Padding	
Starts here ...			Payload of IP datagram	

Used also in IPv6 (called "Next header")

**Protocol field** (8 bits): describes which higher layer protocol is used (TCP, UDP, SCTP ...). The header of this protocol is located at the beginning of the IP datagram payload.

## IPv4 header structure (8)

Version	IHL	Type of Service	Total length of IP datagram	
Identification			Flags	Fragment offset
Time-to-live	Protocol		Header checksum (for error control)	
Source IP address				
Destination IP address				
Options				Padding
Payload of IP datagram				

**Header checksum** (16 bits): used for error control (if used, routers along the path have to recalculate the checksum).

This kind of error control is not used in IPv6 (since the same error control function is offered by TCP - and even UDP).

## IPv4 header structure (9)

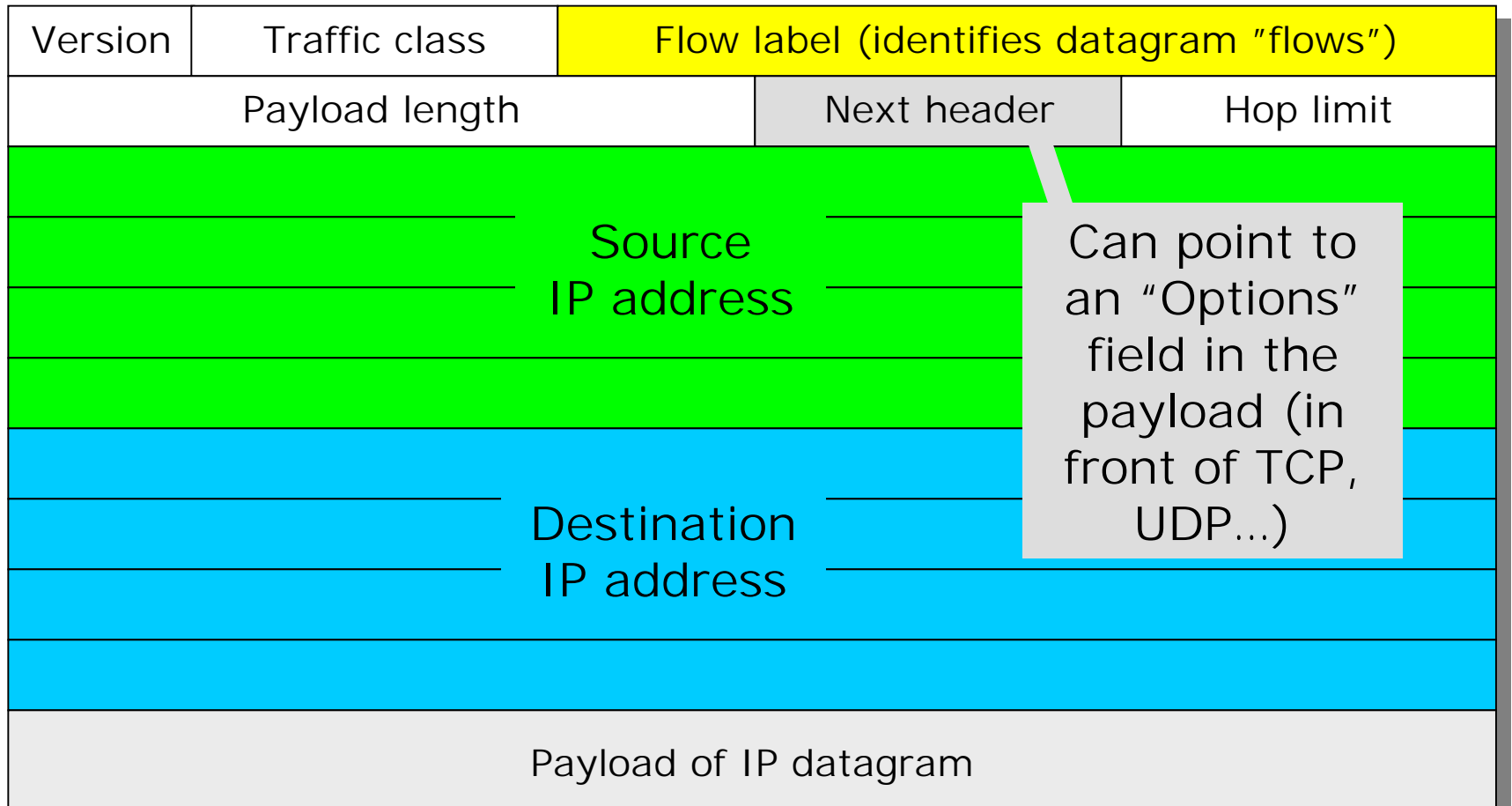
Version	IHL	Type of Service	Total length of IP datagram	
Identification			Flags	Fragment offset
Time-to-live	Protocol		Header checksum (for error control)	
Source IP address				
Destination IP address				
Options				Padding
Payload of IP datagram				

Source and destination IP address (32 bits each): note that these addresses are not changed in routers along the route.

In IPv6: the addresses are  $4 \times 32 = 128$  bits long!



# IPv6 header structure



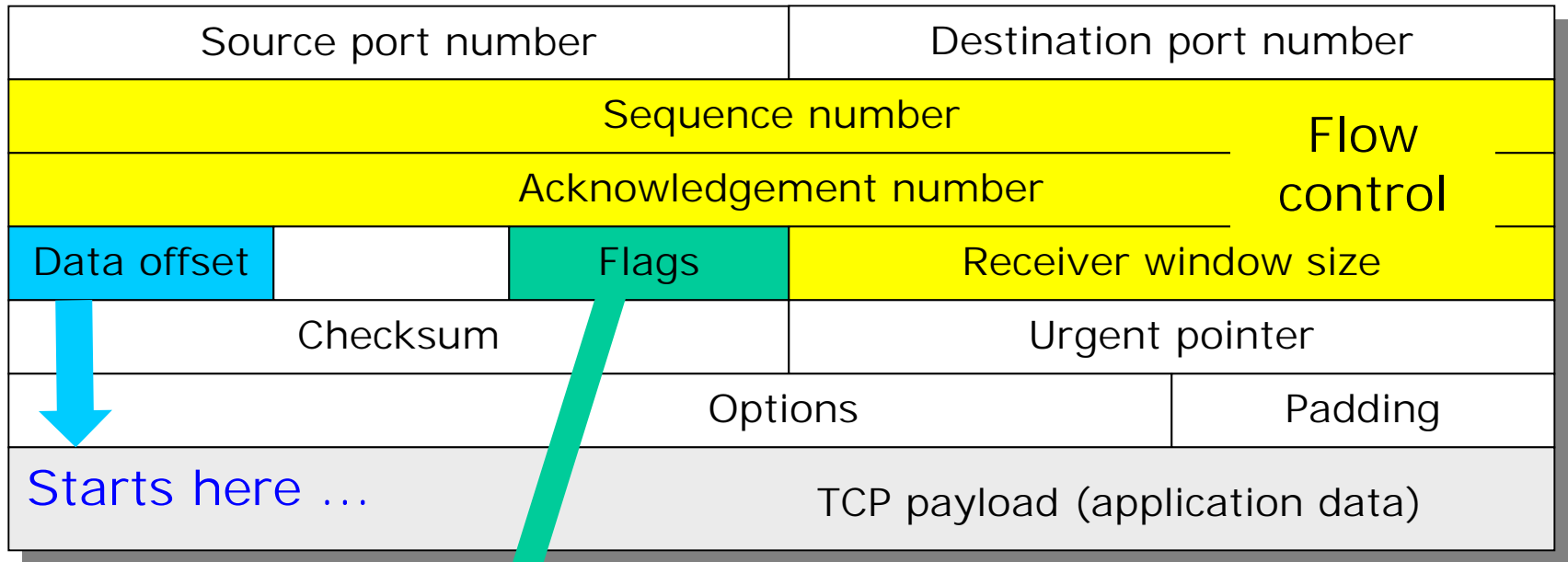
# UDP header structure

Source port number	Destination port number
Length of UDP content (incl.header)	Checksum
UDP payload (application data)	

Two functions of UDP:

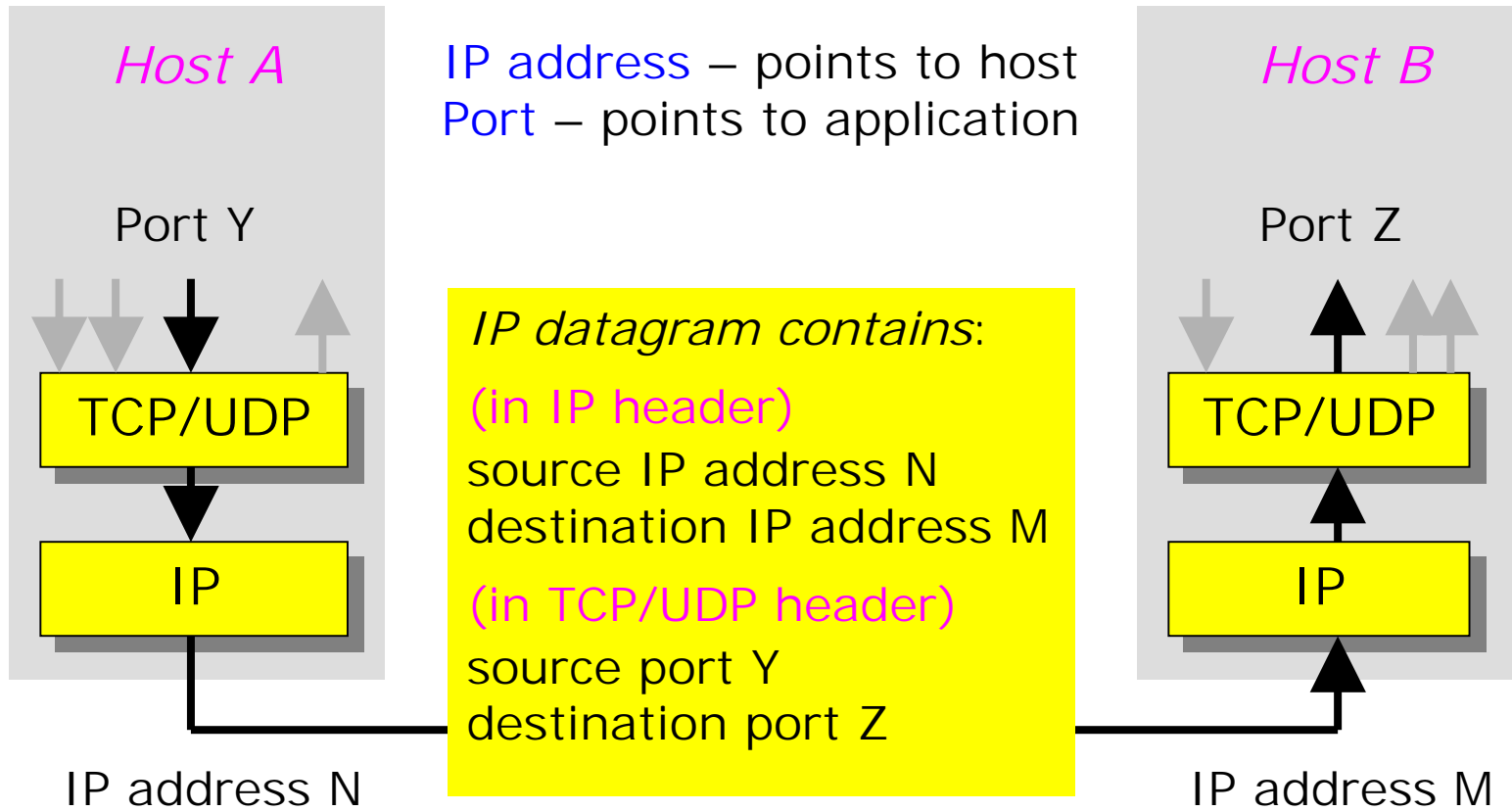
- Application multiplexing (using port numbers)
- Error control (using checksum)

# TCP header structure



Flags are one-bit indicators (SYN, ACK, FIN ...) used for simple signalling (TCP connection setup and teardown)

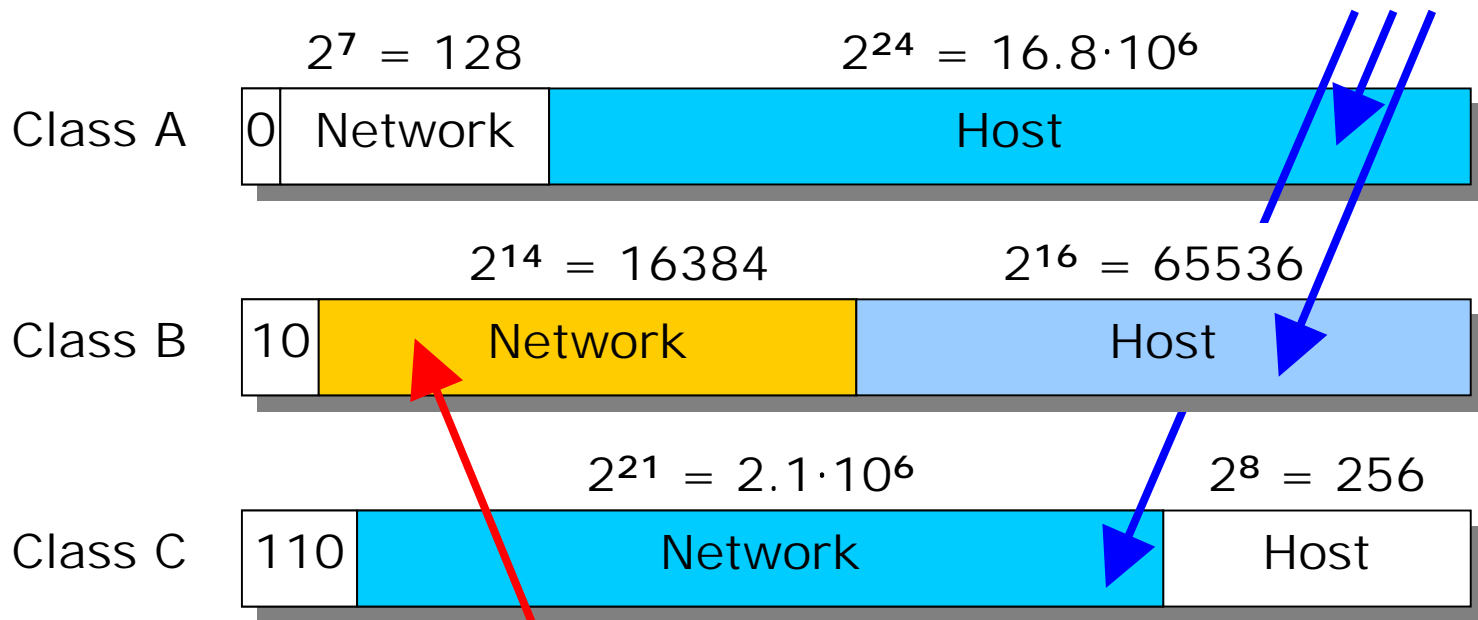
# IP address vs. port number



# IPv4 address structure

Hierarchical structure:

unnecessary capacity



running out of addresses => IPv6 is needed !

Flat structure would provide  $2^{32} = 4.3 \cdot 10^9$  IP addresses

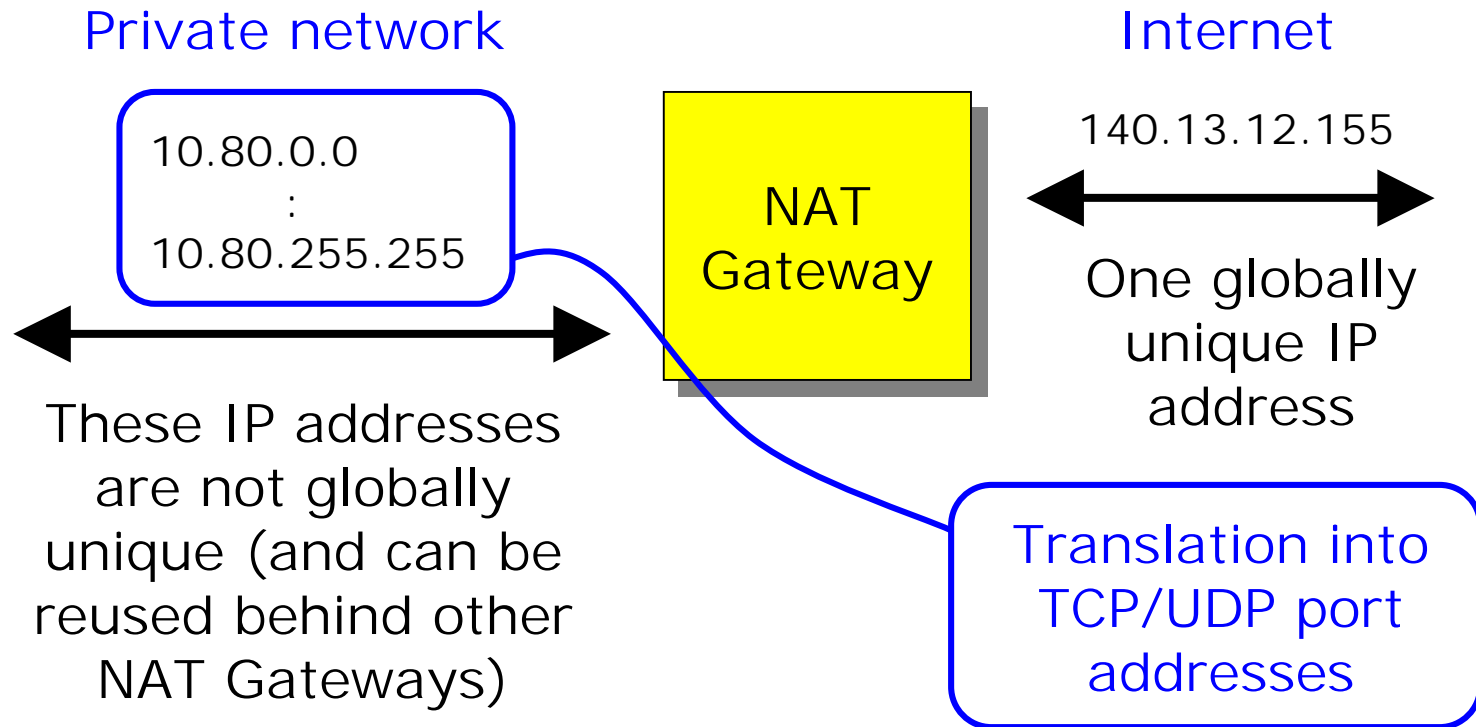
IPv6 provides  $2^{128} = 3.4 \cdot 10^{38}$  IP addresses !

# Ways of increasing address space

1. Group several "Class C" networks into a single larger IP network with larger IP addressing space (> 256 addresses)
2. Use NAT (Network Address Translation) for translating between TCP/UDP port addresses (on the Internet side) and private IP addresses (on the private subnetwork side)
3. Use dynamic IP addressing for temporary usage or for mobile IP terminals
4. Move to IPv6.

# NAT (Network Address Translation)

## Addressing of nodes in private networks



# Dynamic IP address allocation

IP address is allocated **temporarily**:

- address is taken from an address pool
- after usage, address is returned to the address pool

Applications:

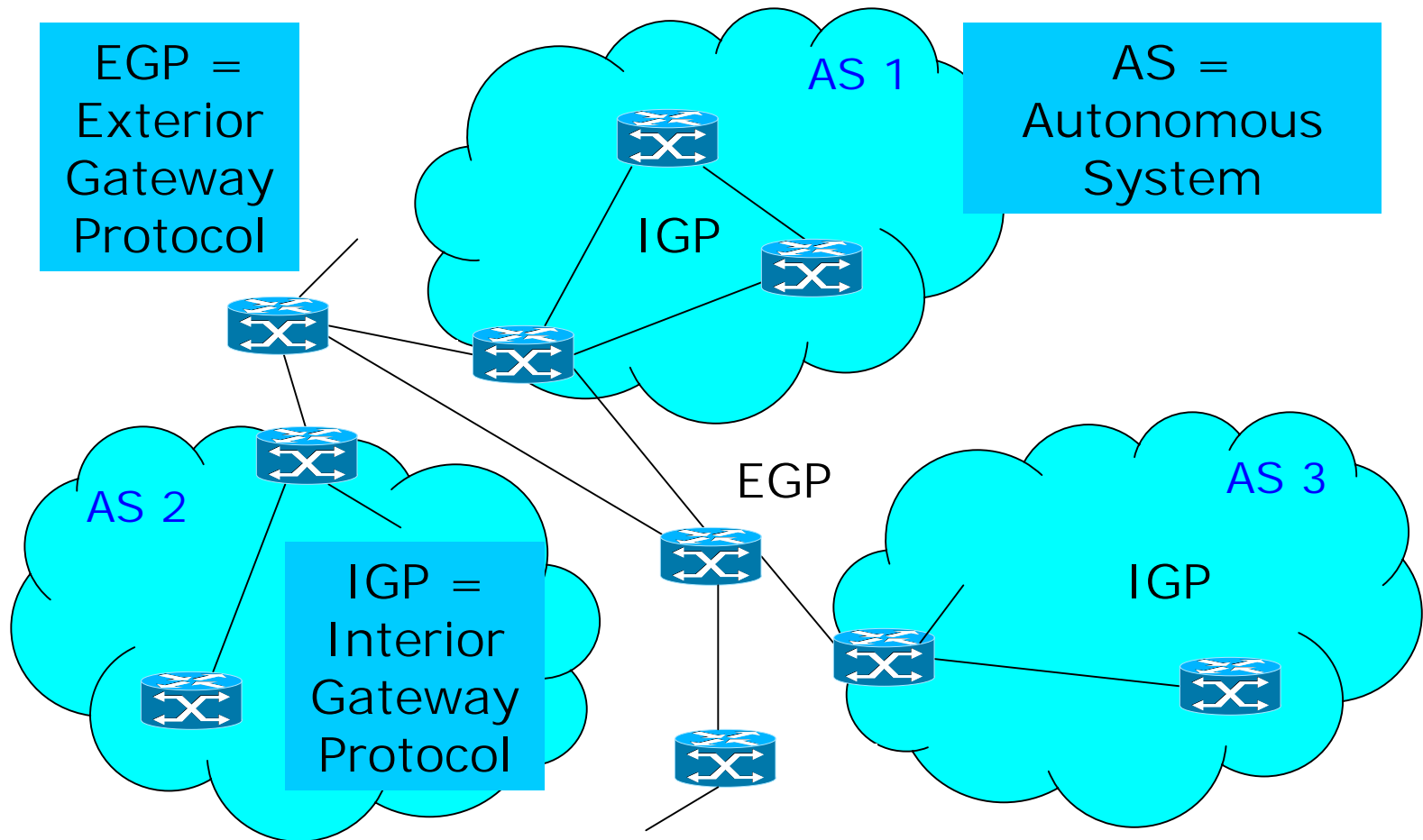
- Dial-up Internet access or ADSL
- GPRS
- Companies with internal network (e.g. LAN)

Protocol used:

- DHCP (Dynamic Host Configuration Protocol, RFC 2131)

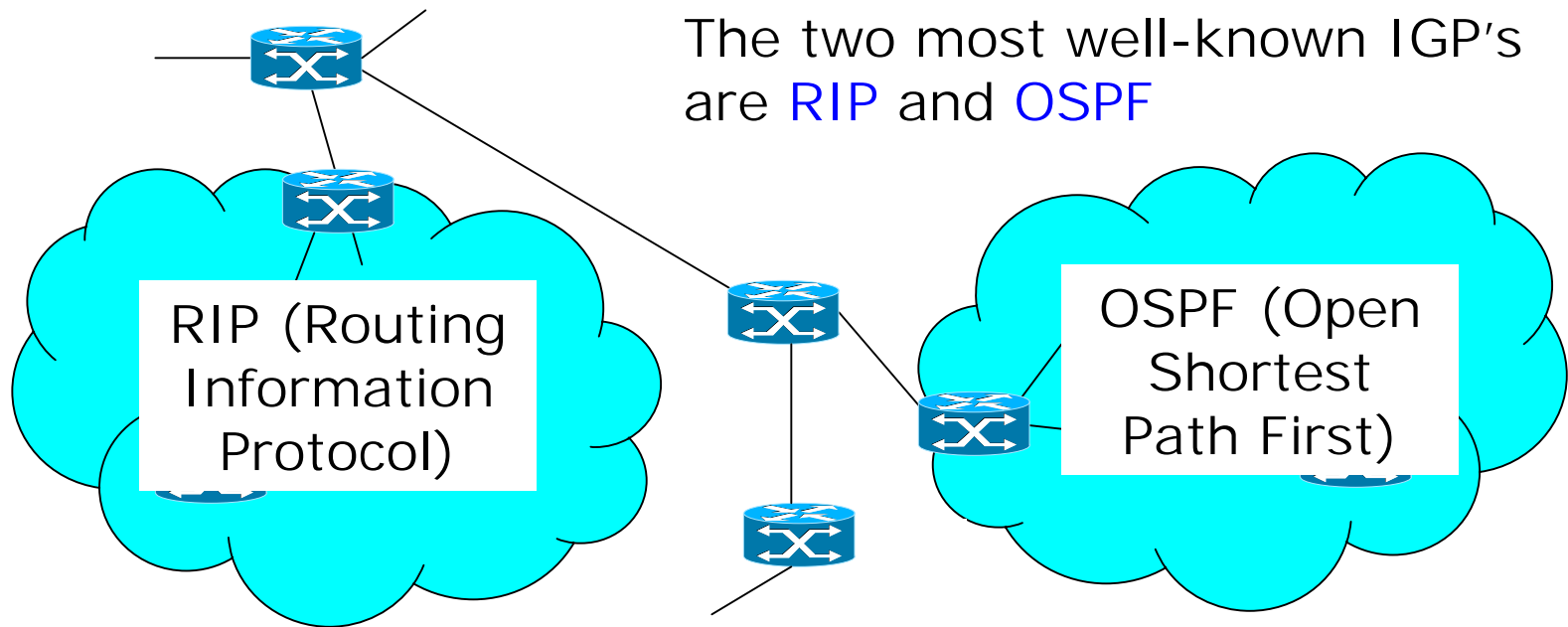


# Hierarchical structure of Internet



# Routing protocols in Internet

In practice, there is worldwide only one very complex EGP, namely **BGP** (Border Gateway Protocol)



# RIP vs. OSPF

RIP is a **distance vector** routing protocol, where neighbouring routers exchange routing information.

RIP is one of the oldest IGPs and is still widely used today.

RFC 1723

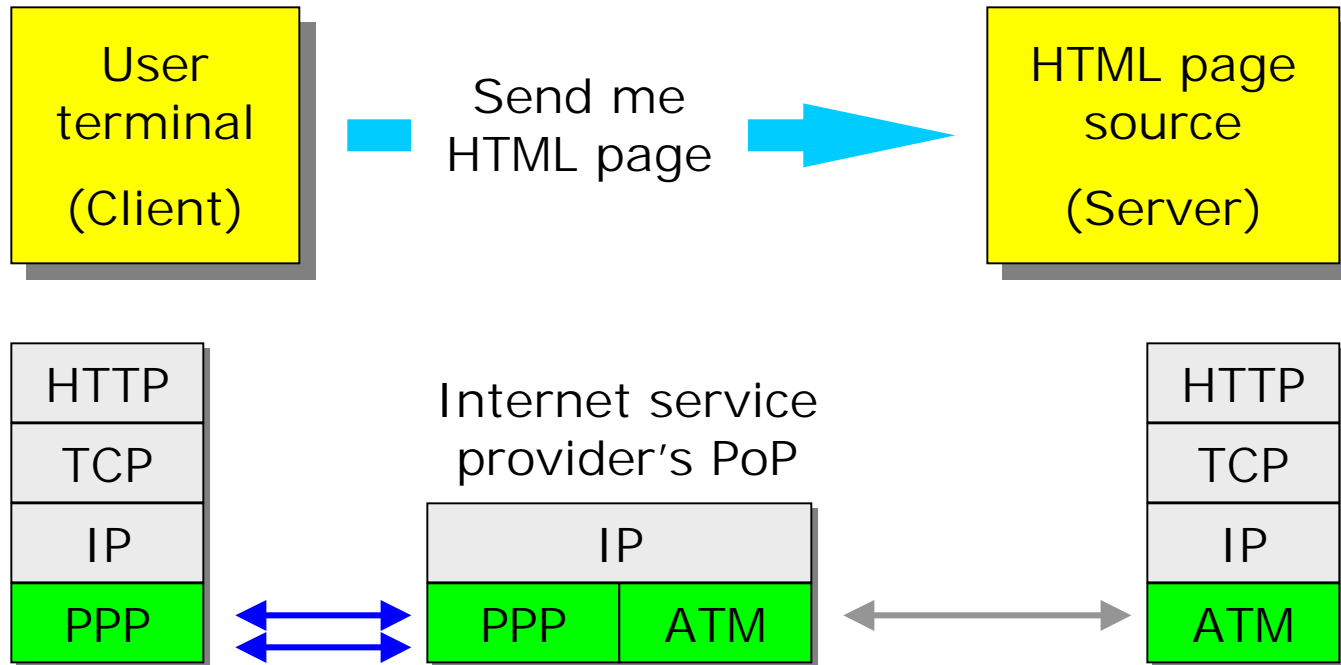
OSPF is a **link-state** routing protocol, where routers construct a complete topological map of the entire autonomous system.

Autonomous system can be hierarchically structured into smaller "networks".

Open => publicly available  
(not like Cisco's EIGRP)

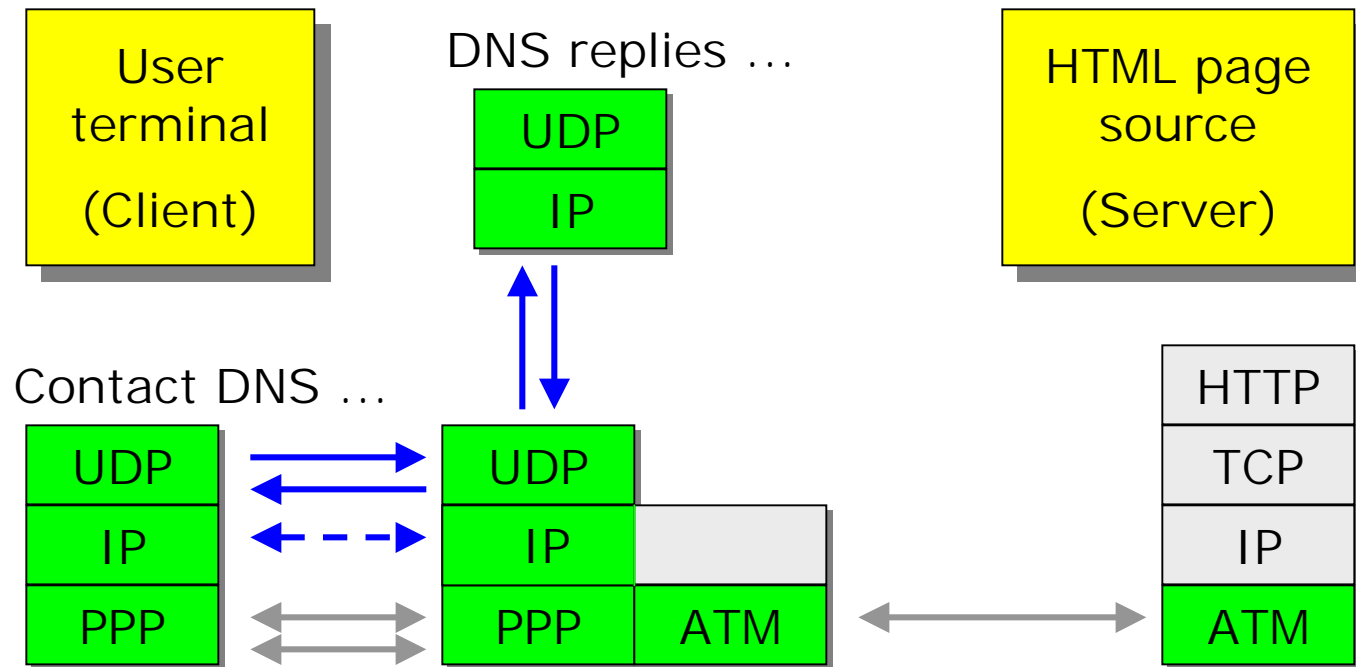
RFC 2178

# Example: downloading HTML page (1)



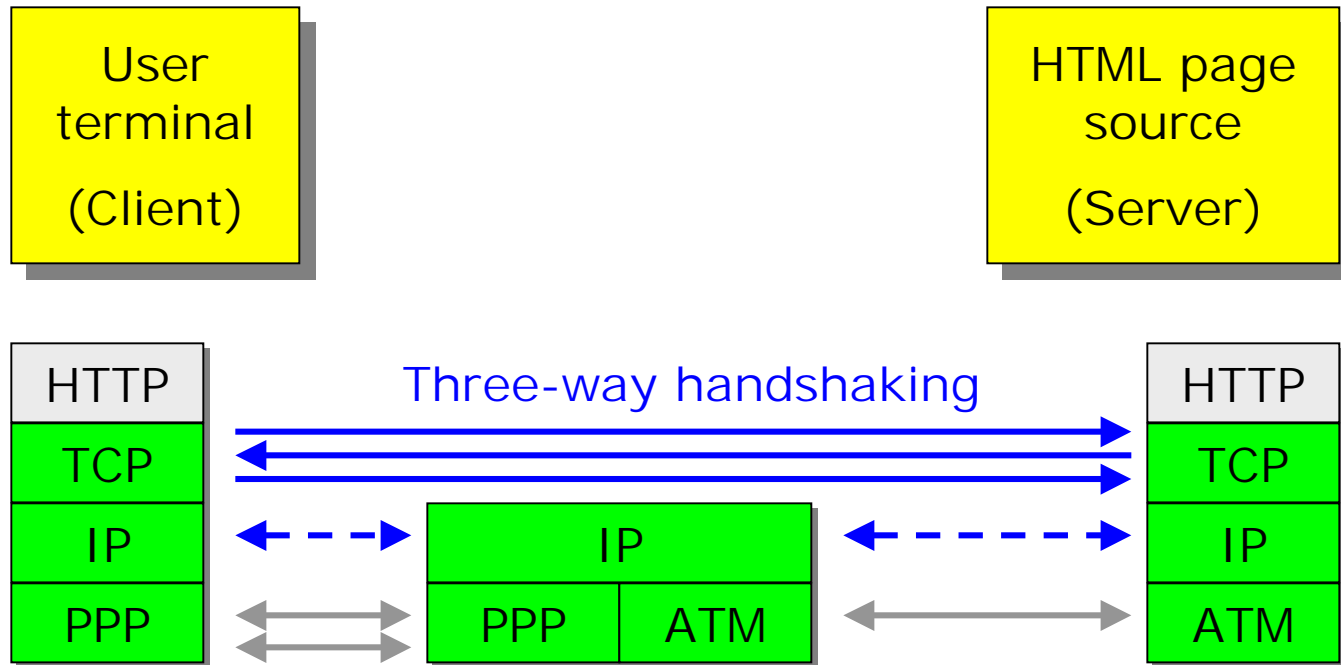
Modem connection and PPP link between user terminal and ISP's Point of Presence (PoP) is established. User terminal is given IP address (dynamic allocation).

## Example: downloading HTML page (2)



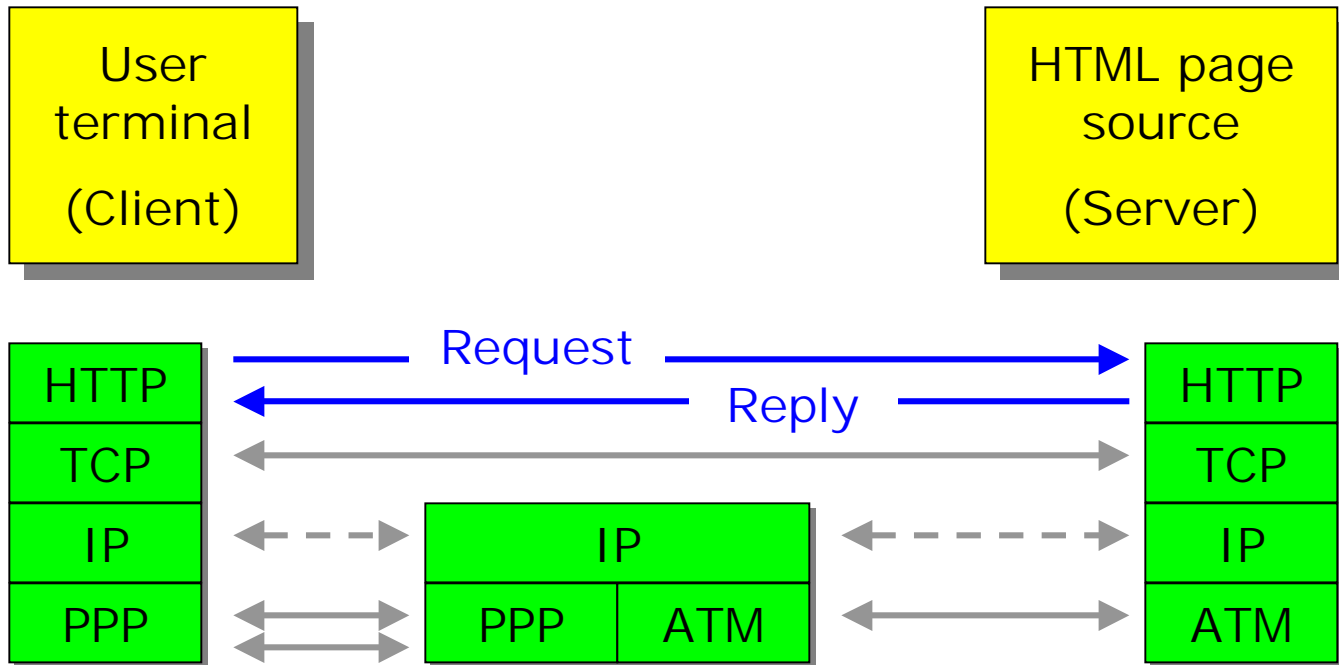
DNS performs translation between URL and IP address of server (only the latter is used for routing IP packets to the server).

## Example: downloading HTML page (3)



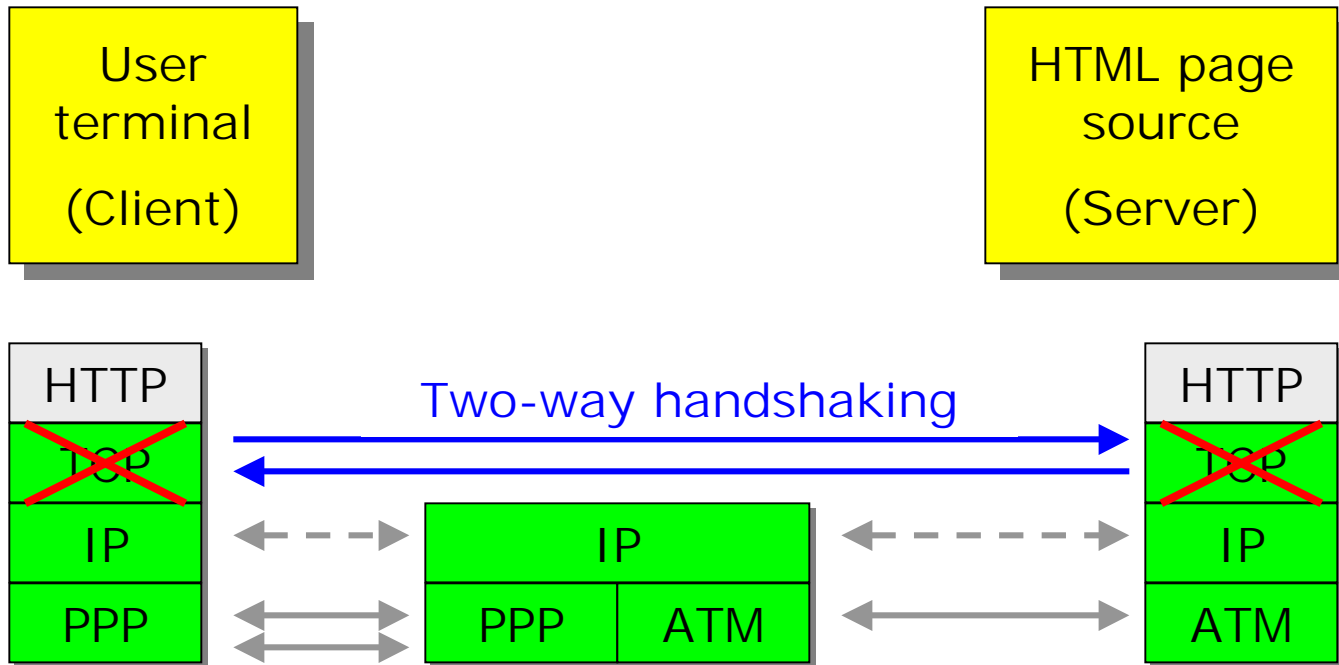
TCP connection is set up. Note that IP packets can be routed over different bearer networks (like ATM as above) and do not necessarily follow the same path.

## Example: downloading HTML page (4)



HTTP request (get HTML page) is sent to server. HTTP reply (including HTML page) is returned in a "200 ok" message.

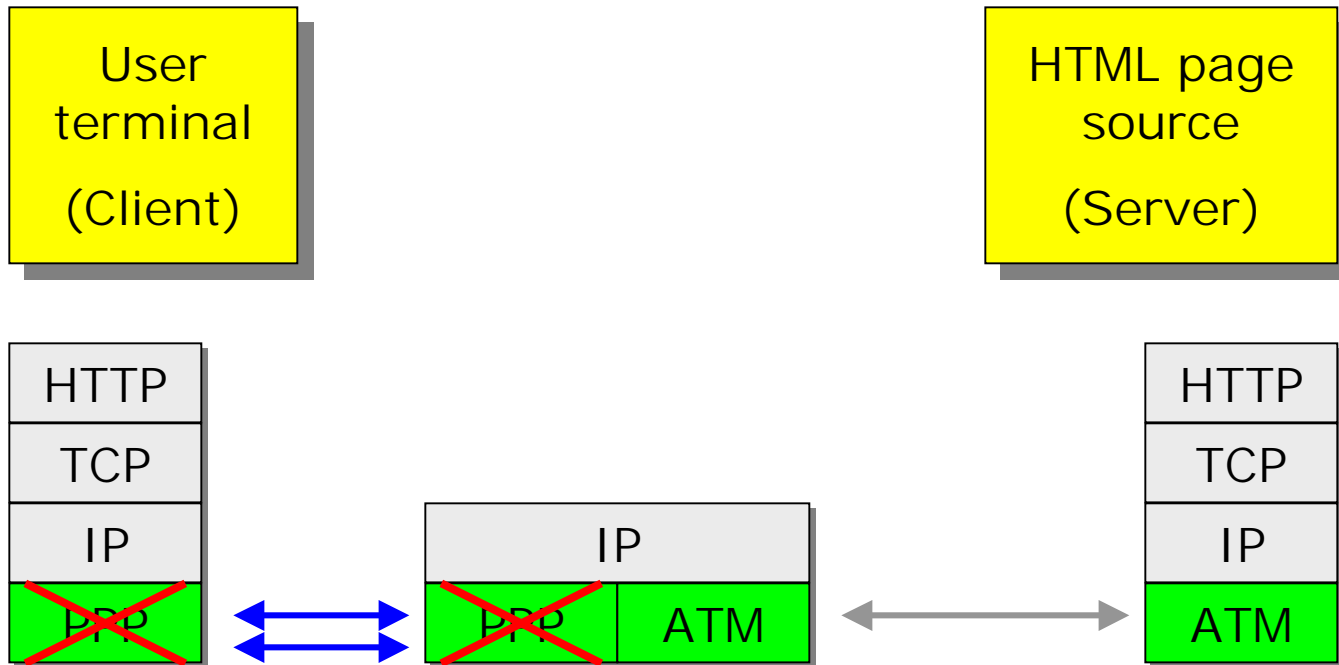
# Example: downloading HTML page (5)



If the client has no more requests, the TCP connection is cleared.



## Example: downloading HTML page (6)



When requested by the client, the PPP and modem connections are cleared. (Bearer connections within the Internet backbone are naturally not cleared.)

# Strong points of IPv6

Larger IP address space

( $3.4 \cdot 10^{38}$  IP addresses available)

Fixed IP datagram header length (no variable length options field ...) and better way to handle options

More simple (and therefore faster) header processing; no checksum checking or fragmentation

Real-time service support (using "flow label" and "traffic class" fields)