# UNIVERSITY OF CAGLIARI

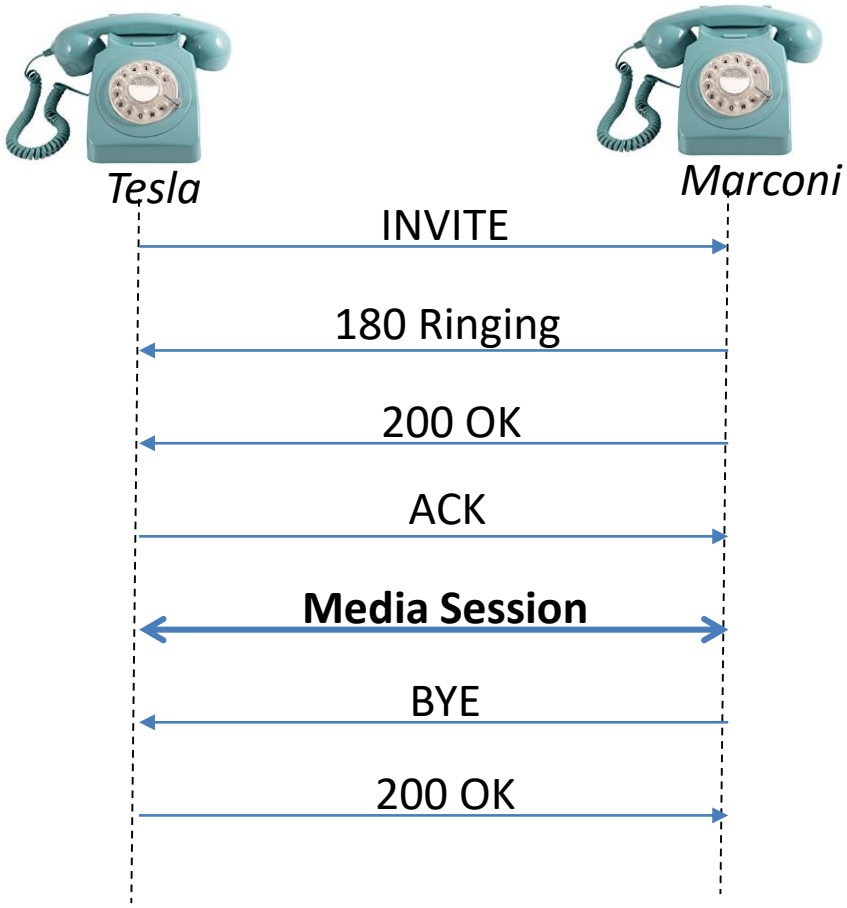
DIEE - Department of Electrical and Electronic Engineering

# Infrastrutture ed Applicazioni Avanzate nell'Internet

## Application protocols: SIP and WebRTC

SIP: Understanding the Session Initiation Protocol, Fourth Edition (Telecommunications) by Alan B. Johnston (2015-11-30), Alan B. Johnston, Hartech house, ISBN-13: 978-1608078639

# SIP (Session Initiation Protocol): simple session




- Two devices that directly communicate each other (e.g., two softphones)
- Each one knows the IP of the other
- SIP is a text-encoded protocol (human – readable)
- The INVITE message is intended to call the other party

# SIP: simple session

*Tesla* *Marconi*

INVITE

*Address of the one that originated the message, plus the port and the transaction ID*

*Request URI*

```
INVITE sip:Marconi@radio.org SIP/2.0
Via: SIP/2.0/UDP lab.high-voltage.org:5060;branch=z9hG4bKfw19b
Max-Forwards: 70
To: G. Marconi <sip:Marconi@radio.org>
From: Nikola Tesla <sip:n.tesla@high-voltage.org>;tag=76341
Call-ID: j2qu348ek2328ws
CSeq: 1 INVITE
Subject: About That Power Outage...
Contact: <sip:n.tesla@lab.high-voltage.org>
Content-Type: application/sdp
Content-Length: 158
```

*Max num of forwards*

*Origin and destination of the call (routing based on the Request URI as this may change)*

*To identify the session*

*SDP (Session Description Protocol) in the body*

*SDP in the body*

```
v=0
o=Tesla 2890844526 2890844526 IN IP4
s=Phone Call
c=IN IP4 100.101.102.103
t=0 0
m=audio 49170 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

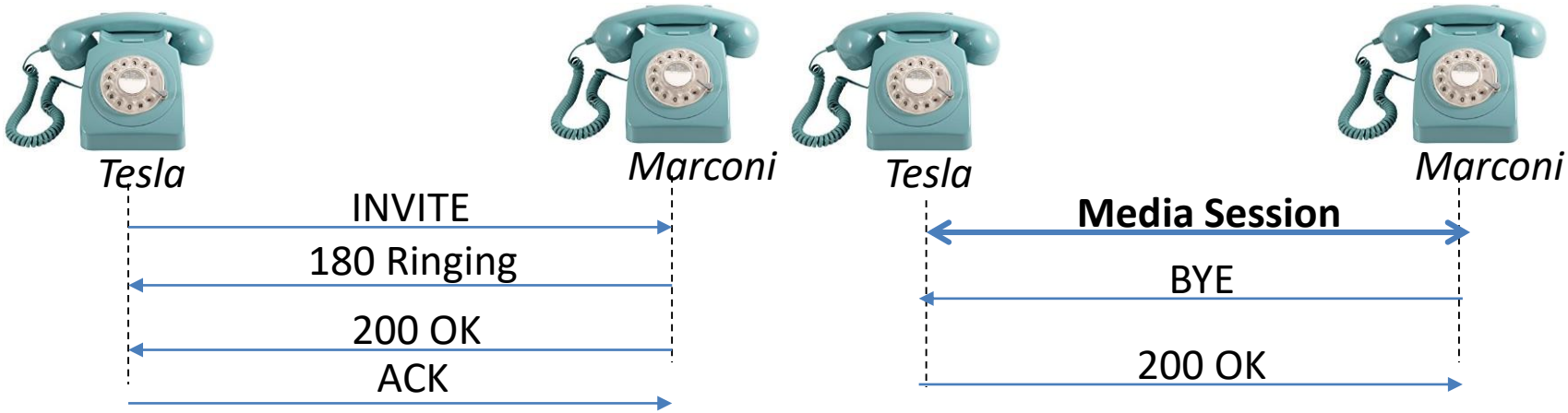
# SIP: Session Initiation Protocol


*Three digits are used to inform about the response meaning (the type is decided by the first digit), 1 is informative, any phrase can be used instead of Ringing*

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP lab.high-voltage.org:5060;branch=z9hG4bKfw19b
 ;received=100.101.102.103
To: G. Marconi <sip:marconi@radio.org>;tag=a53e42
From: Nikola Tesla <sip:n.tesla@high-voltage.org>;tag=76341
Call-ID: j2qu348ek2328ws
CSeq: 1 INVITE
Contact: <sip:marconi@tower.radio.org>
Content-length: 0
```

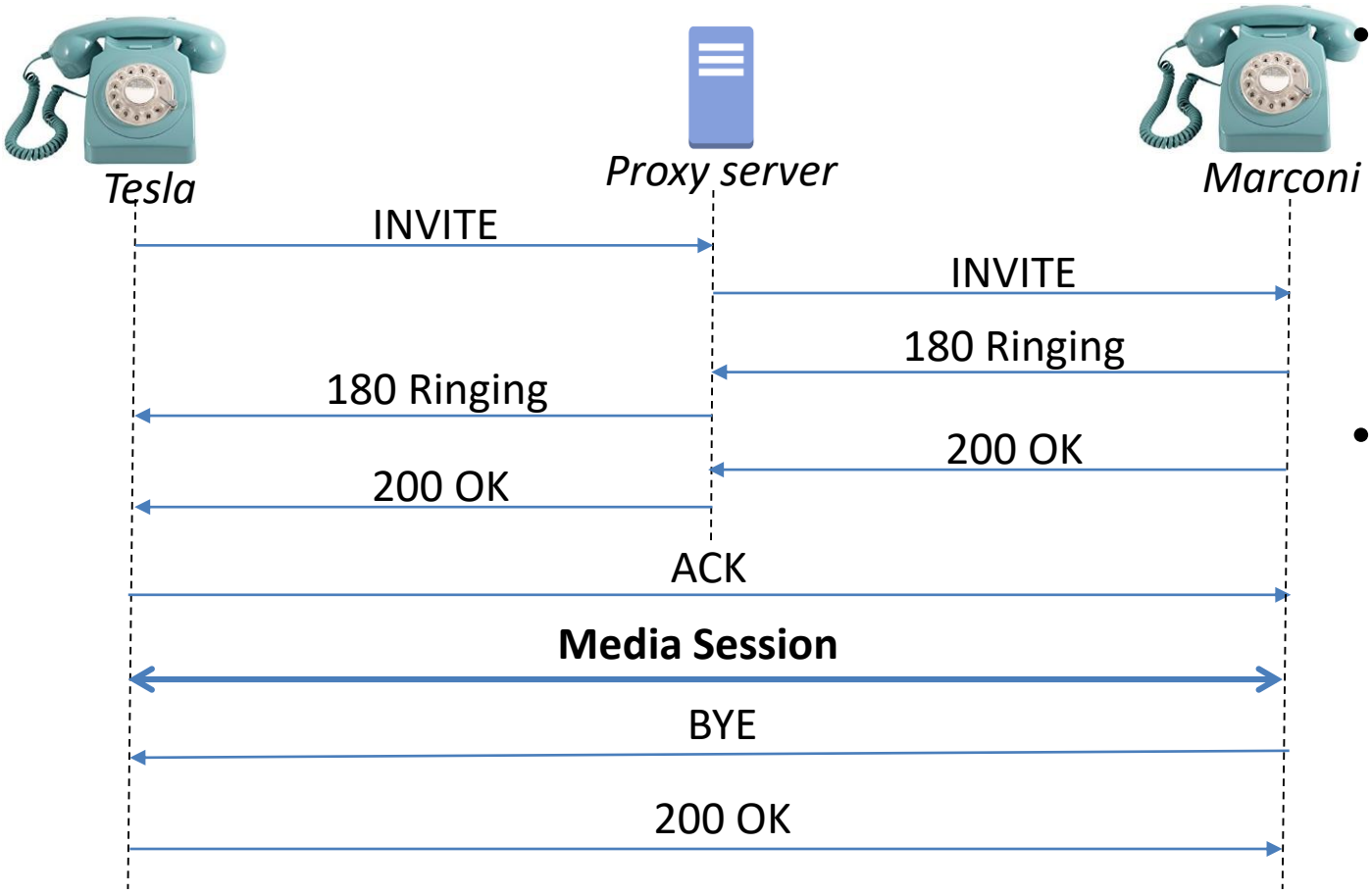
*Many fields are repeated from the INVITE method*

# SIP: Session Initiation Protocol



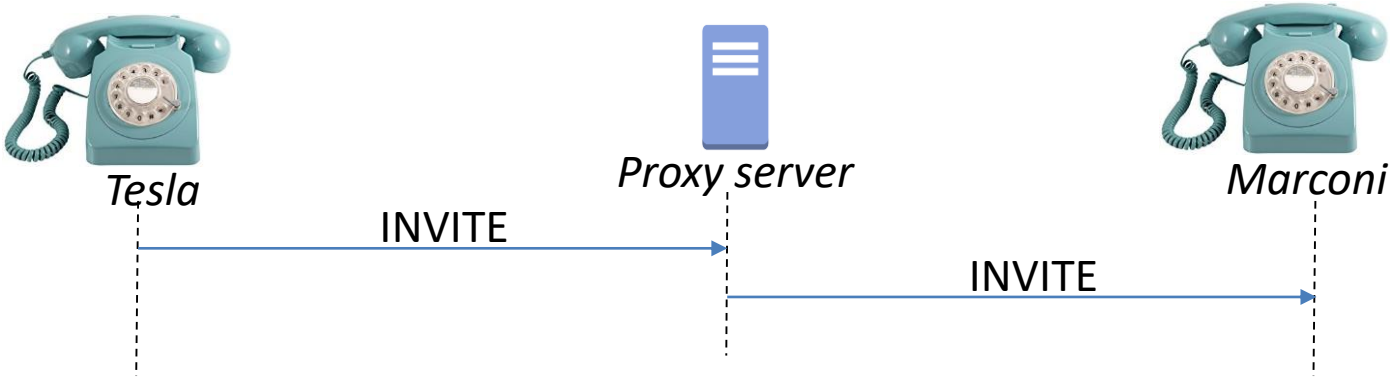

- When the receiver decides to accept the call, the "200" message is sent
  - This also means that the media for the call is ok
- Finally an ACK is sent by the originator
  - Then the media session starts, typically using RTP protocol
- Bye and relevant ACK are then sent to terminate the session

# SIP: call with a proxy server




- Most of times the hosts do not know the IP address or it is not used to identify the user phone
- Typically, the user has an address that would identify her wherever she is (see email address)
  - This is the SIP URI
  - DNS lookups are used

# SIP: call with a proxy server

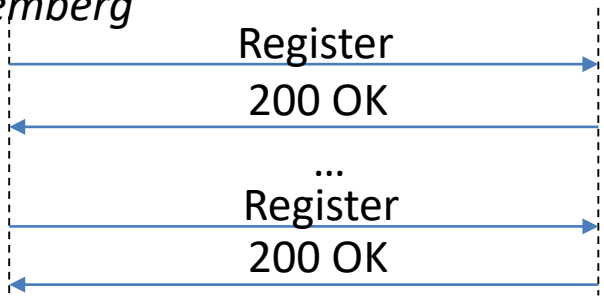



- User URI, named also address of record (AOR), required lookups that give one or more addresses of end devices
  - Typically in the To and From headers
- Device URI, which does not require any database lookups
  - Typically in the contact header
- As Tesla does not know the Marconi address
  - DNS lookup for the proxy address for Marconi User URI (the one of marconi@radio.example.org)
  - The Invite is sent to the proxy
  - The proxy performs a database lookup to get the address of Marconi
  - The Invite is sent to Marconi address with the additional via header field to add its address
  - Marconi understands the Invite has been sent through the proxy and the response (180 ringing) is then sent to the proxy
  - The same happens for the 200 OK
  - Afterwards, the messaging is carried out end-to-end without the proxy

# SIP: Registration process

*Heisemberg*

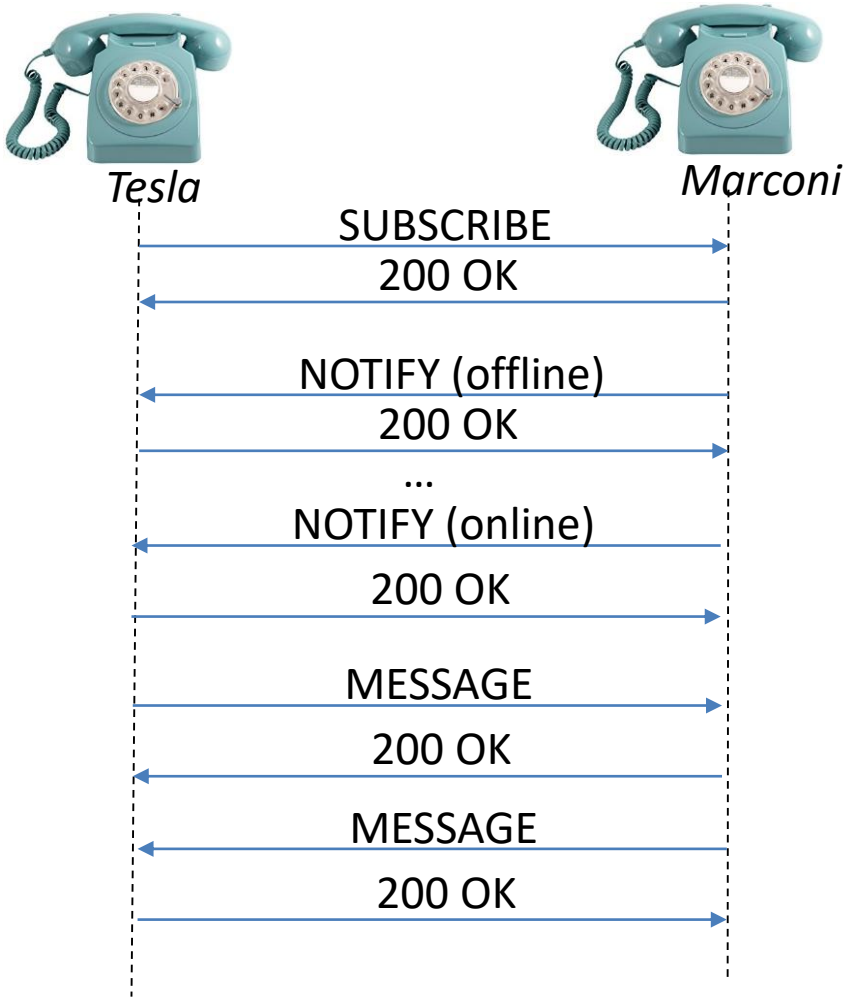
*Registrar server*




```
REGISTER sip:registrar.munich.de SIP/2.0
Via: SIP/2.0/UDP 200.201.202.203:5060;branch=z9hG4bKus19
Max-Forwards: 70
To: Werner Heisenberg <sip:werner.heisenberg@munich.de>
From: Werner Heisenberg <sip:werner.heisenberg@munich.de>
 ;tag=3431
Call-ID: 73764291
CSeq: 1 REGISTER
Contact: sip:werner.heisenberg@200.201.202.203
Content-Length: 0
```

- Objective: update the binding between the User URI and the Device URI
  - User URI is the one printed in the business cards and published on the web
  - In the Register this is conveyed in the To header
  - The device URI is in the Contact header -> this is the device the user is currently connected to
- When a proxy received an Invite on this User URI, it enquires the register server to get the contact information
- This process is very similar to the wireless phone system
  - The phone sends the identity to the base station (BS), which then forwards the location and phone number to a home locator register (HLR)
  - When a call is received the mobile switching center enquires the HLR database

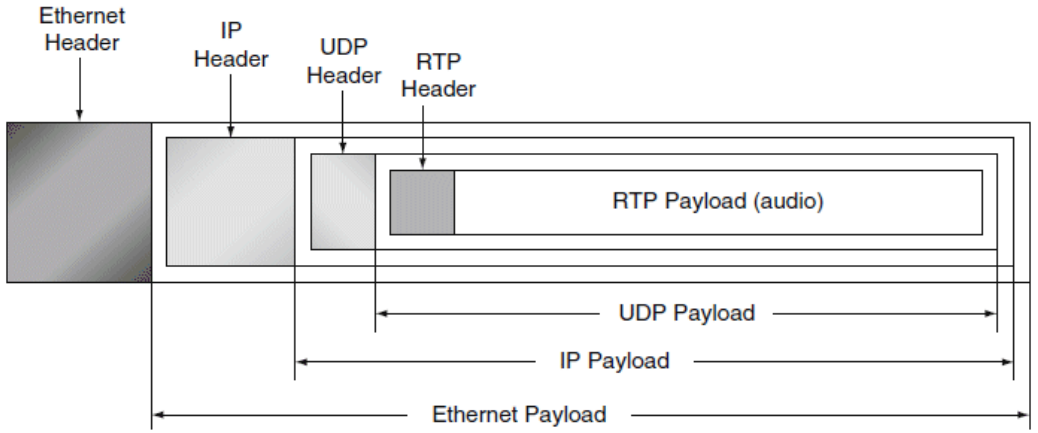
# SIP: presence and instant message




- Presence message: to know the status of the device
- It is thought as a long-term relationship between two devices
- Message is used to send a message and is not considered as a part of a flow with other messages

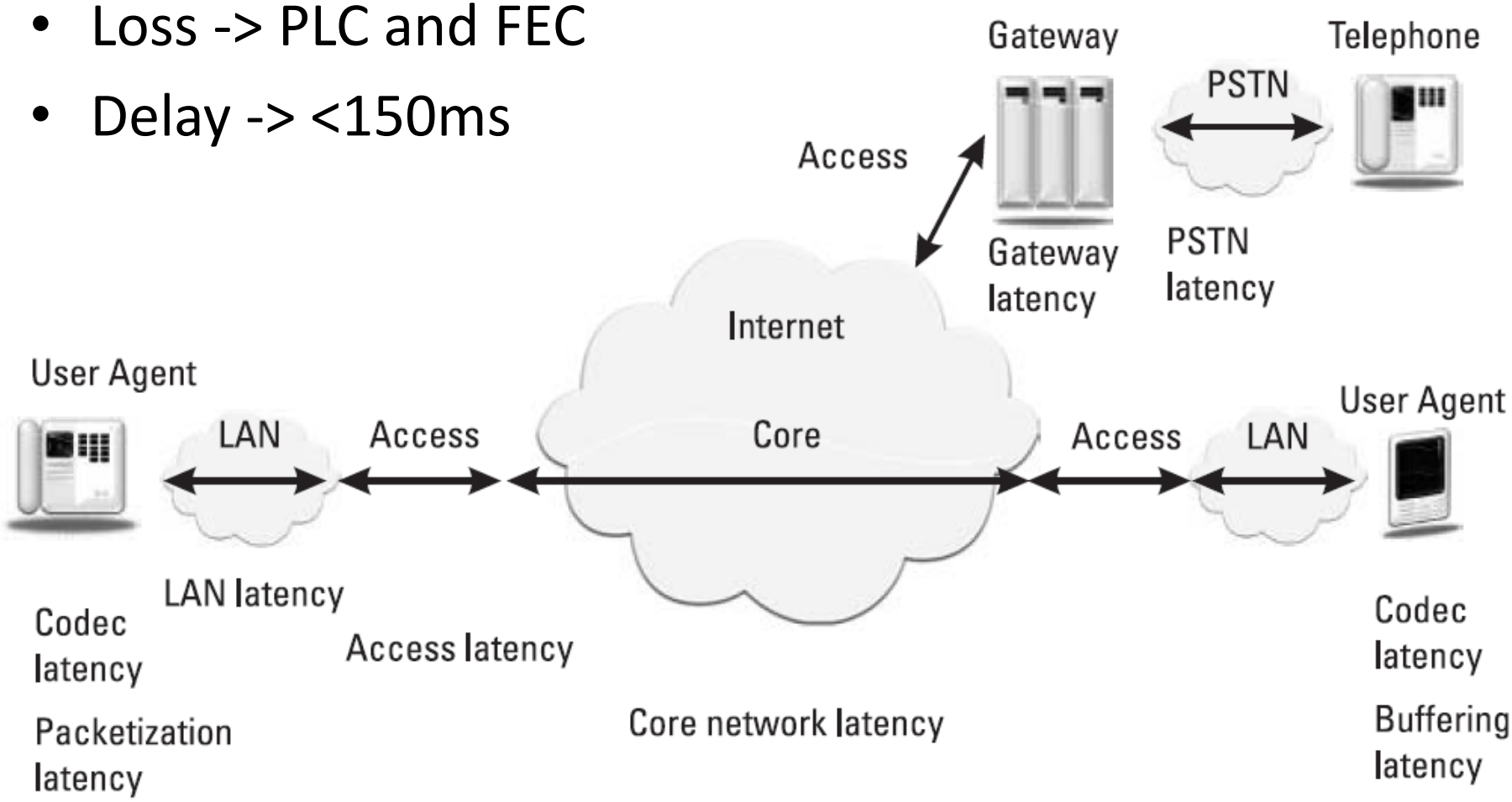
# Media transport

- RTP – Real-Time Transport Protocol (started in 1992)
  - Used by both SIP and H.323
  - Defined by the IETF
  - No QoS guaranteed, but provides tools to monitor (e.g., packet loss, delay, out-of-order)
- Media processing steps and RTP
  - Coding (payload type field of RTP, rate in SDP)
  - Packetization (often 20-30ms packets, overhead to be taken into account)
  - Transport -> UDP is used
  - Depacketization
  - Buffering
  - Decoding
  - Playback

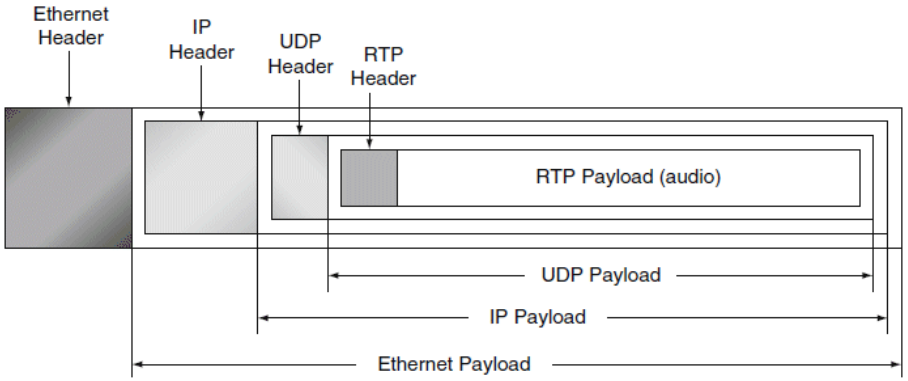


# RTP: provided quality

- Loss -> PLC and FEC
- Delay -> <150ms



# RTP: fields (12 bytes)



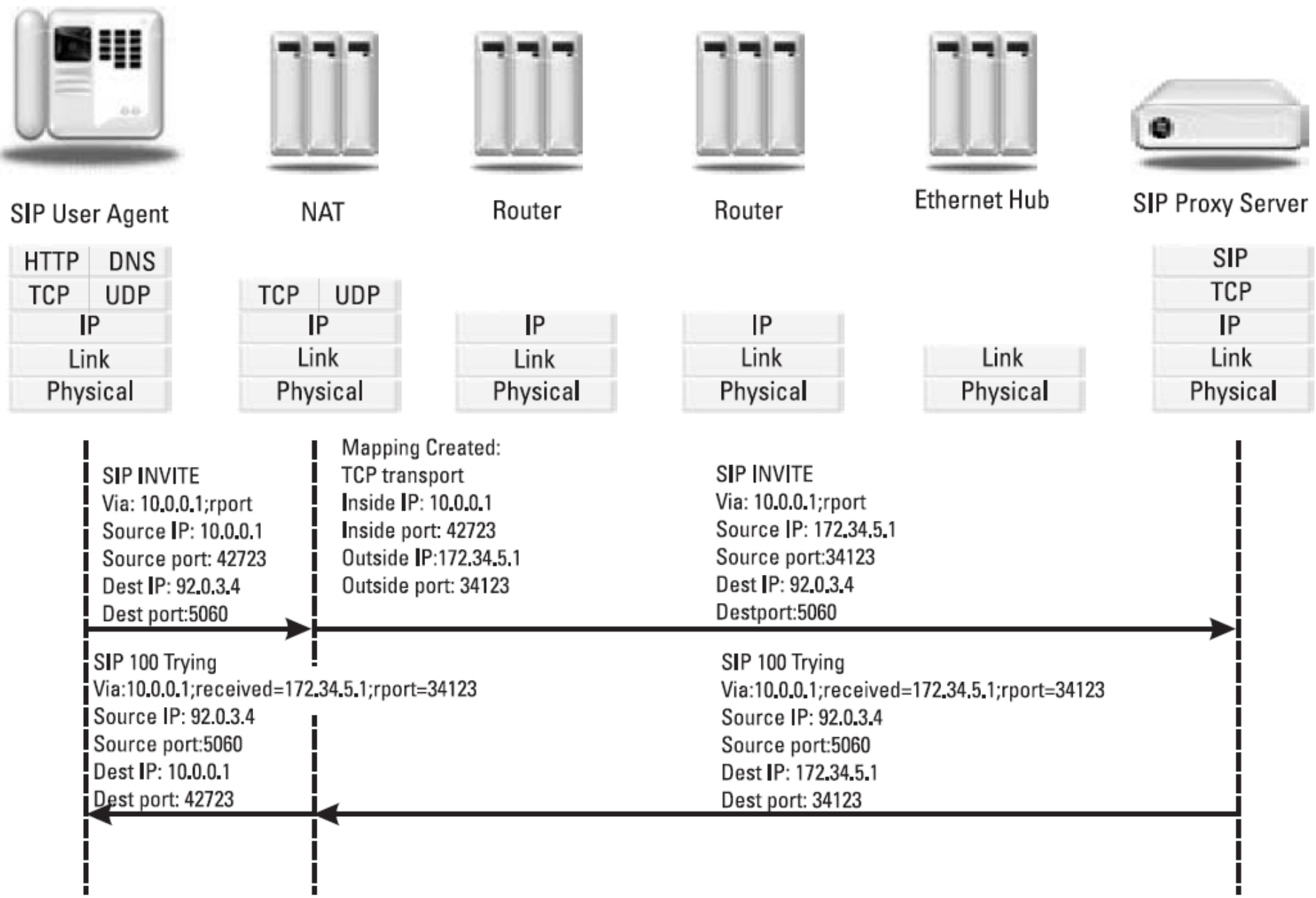

- The important ones are
  - Payload type: which codec is used
    - It allows for changing the used codec even if not agreed through the SDP
  - Sequence number: incremented for each RTP packet
    - It allows for detecting losses
  - Timestamp: it indicates in relative terms the time when the payload was sampled
    - It allows for detecting the jitter
  - SSRCI (Synchronization source identifier): 32 bit field to identify the sender
    - No one can enter in a communication if this is unknown

# RTCP

- Real-time Control Protocol
  - It is used to send quality *reports* about an RTP session
    - Number of packets sent and received
    - Number of packets lost
    - Packet jitter
  - Many reports are defined, but the sender and receiver reports are the most used
  - The rate of reports is constant whatever the number of parties (typically one packet every 5 seconds)
  - Each session is unidirectional

# RTP compression and mixing

- Consider a low-bitrate codec of 12.1kbps with 20ms of packetization time over RTP, UDP, IPv4 and Ethernet
  - What is the overhead?
- CRTP (compression RTP) is then often used
  - Only the RTP header, as many fields change rarely
  - It is not only used to reduce the bitrate but also to reduce serialization delay in low bitrate lines
    - What is the serialization delay?
- Conferencing
  - N-1 audio flows are mixed together
  - The SSRC of each media stream included will be copied into the contributing SSRC field


SIP User Agent
NAT
Router
Router
Ethernet Hub
SIP Proxy Server
HTTP
DNS
TCP
UDP
IP
Link
Physical
TCP
UDP
IP
Link
Physical
IP
Link
Physical
IP
Link
Physical
Link
Physical
SIP
TCP
IP
Link
Physical
SIP INVITE
Via: 10.0.0.1;rport
Source IP: 10.0.0.1
Source port: 42723
Dest IP: 92.0.3.4
Dest port:5060
Mapping Created:
TCP transport
Inside IP: 10.0.0.1
Inside port: 42723
Outside IP:172.34.5.1
Outside port: 34123
SIP INVITE
Via: 10.0.0.1;rport
Source IP: 172.34.5.1
Source port:34123
Dest IP: 92.0.3.4
Destport:5060
SIP 100 Trying
Via:10.0.0.1;received=172.34.5.1;rport=34123
Source IP: 92.0.3.4
Source port:5060
Dest IP: 10.0.0.1
Dest port: 42723
SIP 100 Trying
Via:10.0.0.1;received=172.34.5.1;rport=34123
Source IP: 92.0.3.4
Source port:5060
Dest IP: 172.34.5.1
Dest port: 34123

# Pros and cons of NAT

- Advantages
  - Addresses the shortage of IP addresses
  - A network can avoid renumbering IP addresses when changing ISP
  - Mngt of IP addresses is easier if the number of IP addresses is not limited
  - Filtering at the NAT router can be easier
  - Any host that does not initiate the Internet connection is not reachable
  - NAT allows the ISP to better subnet the networks of its customers
- Disadvantages
  - It breaks the end-to-end model of the Internet
  - Reachability of any host is no more valid (assumed by many protocols and architectures)
  - It also breaks the transitive reachability of hosts
  - It creates a single point of failure in the connection
  - Multihoming is not allowed (the response should reach the same interface)
  - It does not allow security at the IP layer
  - Well-know ports cannot be used easily
    - For instance for the well-known SIP port 5060
  - NATs must know all the new transport protocols other than TCP and UDP

# NATs and SIP

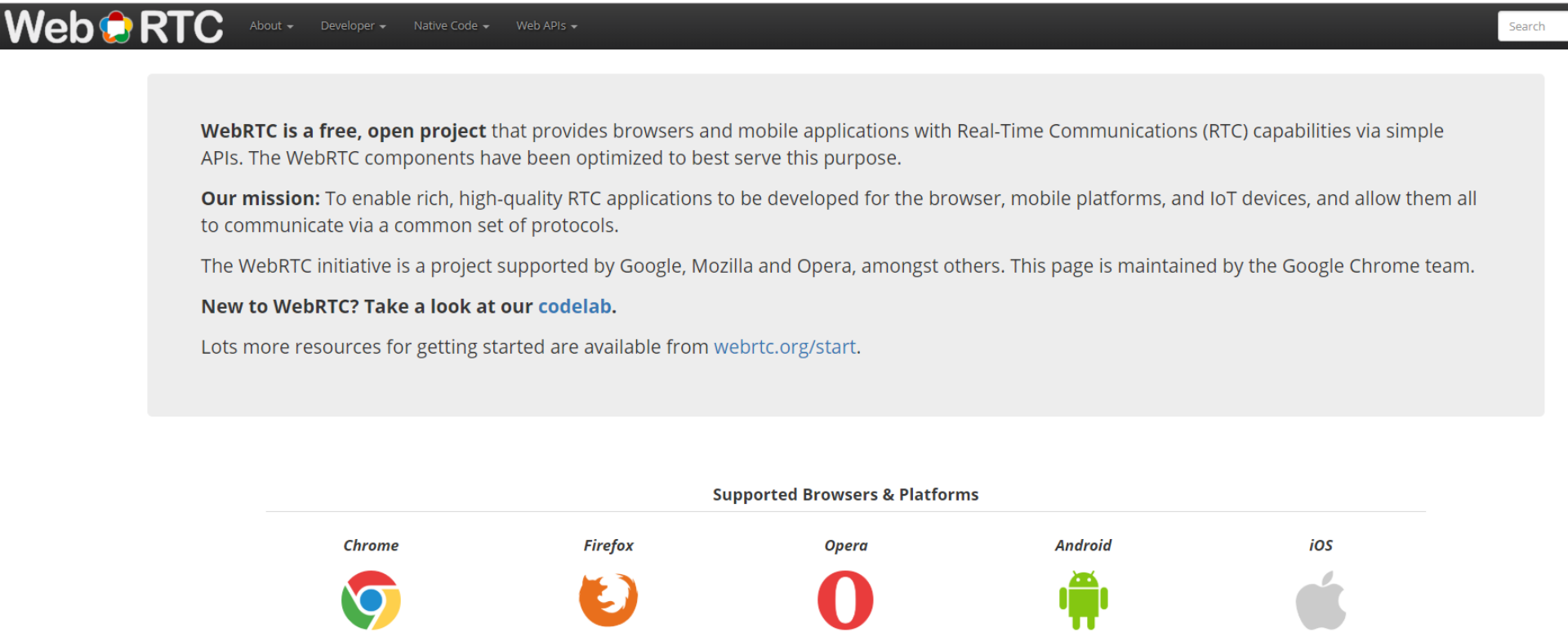
- NAT works well with unencrypted client/server protocols, such as web browsing, e-mail and others
  - Problems with IPSec VPNs, which fails if the checks include the IP address and the port number
  - It causes problems to peer-to-peer protocols and that carry embedded IP addresses and port numbers, such as SIP
- Guidelines for NAT-friendly protocol design in 2002 said that
  - Limit peer-to-peer applications
  - Do not rely on end-to-end IPSec security
  - Use DNS names, not IP addresses
  - Multicast is problematic
  - Avoid session bundles (one session controlling another)
  - Use TCP instead of UDP
- SIP violates most of these recommendations
  - The recommendations arrived too late
  - They assumed IPv6 was going to be deployed widely

# NATs and SIP

- Solution
  - SIP user agents would send test packets to determine if it was behind a NAT
    - This was the STUN protocol (Simple Traversal Utilities for NAT)
    - The STUN clients asks to a STUN server about the mapped address and port the sent packet appeared to be received from
    - With this information the user agent tries to fix the IP addresses and ports in their SIP messages
    - It does not work well with all the cases
      - Use of Interactive Communications Establishment (ICE), which relies on a series of tests based on the STUN protocol

# WebRTC

- It is a standard (IETF and W3C) and industry effort
- It brings multimedia communications into the WWW
- It is a multiplatform open source project

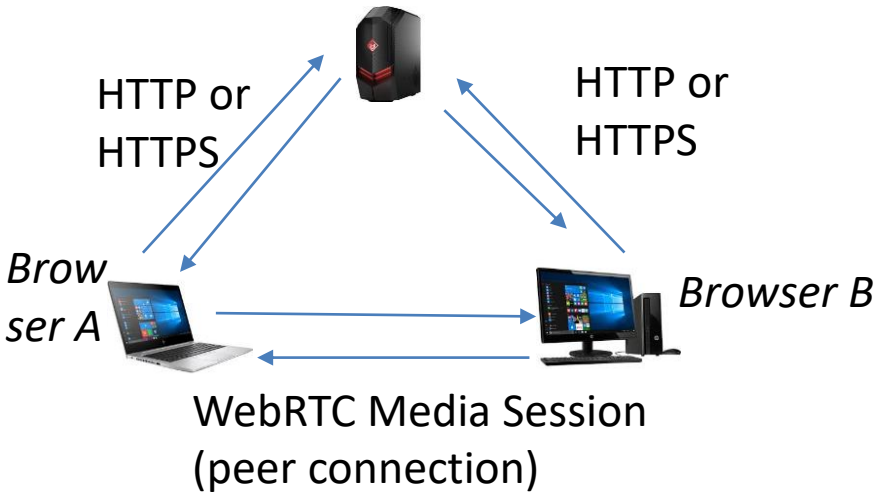


# WebRTC: main features

- Prior to WebRTC
  - Browsers needed a plugin or add-on, which are more and more avoided by browser providers (issues with user skills and malicious software)
  - Requires development specific for each browser
  - Solution: install an external application that is called by the browser
- It overcomes these issues by providing a complete audio and video media stack into the browser
  - Codecs, echo cancellation, packet loss concealment
  - No download, plug-in or add-on needed
  - No need for proprietary protocols or development environments (JavaScript API are standardized and part of the HTML5 standard)
- It defines extensions to the <audio> and <video> HTML tags developed for streaming media, which enable real-time voice and video to be added to any Web page
- The developer writes code in JavaScript using the WebRTC 1.0 APIs and Media Capture and Streams APIs

# WebRTC basics

- It allows for establishing peer-to-peer connections (between web browsers)
  - It was not the case before

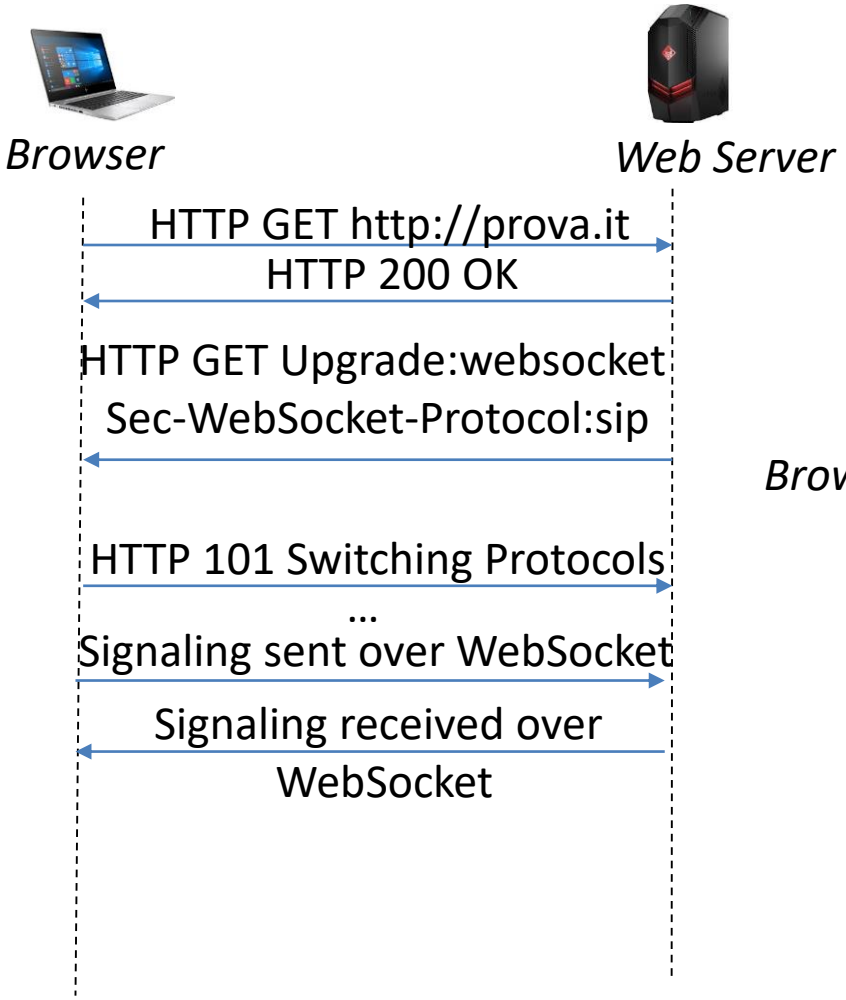


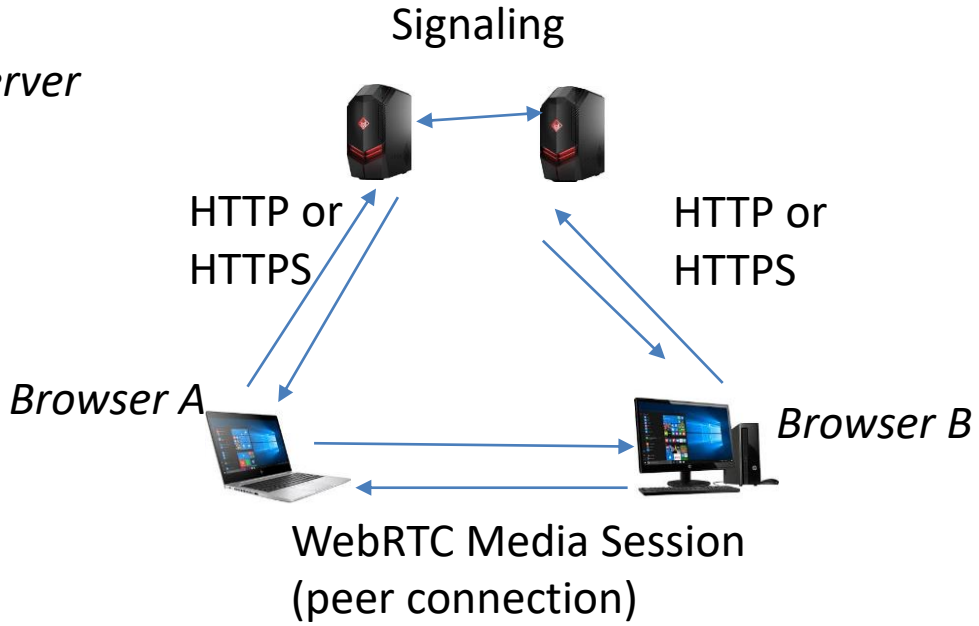

| WebRTC functions |
| --- |
| Audio codecs (Opus and G.711) |
| Audio gain control and packet concealment |
| Media negotiation |
| Video codecs (VP8 and H.264) |
| WebRTC JavaScript APIs (for Peer Connection) |
| Media capture and stream APIs |
| Bandwidth estimation and congestion avoidance |

# WebRTC basics

- We can try with https://appr.tc/
- The look&feel is left to the webpage programmer
- Media exchange is fully standardized, the signaling not. A standard is needed
- Advantages of using SIP
  - Easy integration with existing SIP VoIP service. However few existing SIP systems support the full WebRTC stack -> there is need for a gateway
  - Faster development
- WebRTC signaling only uses HTTP or WebSocket for transport

# WebRTC: signaling and trapezoid connections



# Questions

- What is the user URI and the device URI?
- Why is a proxy  needed in the peer-to-peer communication?
- What is the purpose of the via header?
- What is the meaning of the register request?
- Describe the purpose of packet loss concealment and list some methods
- Why does RTP usually work with UDP transport?
- Explain the purpose of the sequence number and SSRC fields in RTP packets
- Calculate the bandwidth required for a codec operating at 7.5kbps, 25ms packetization time, assuming transport over UDP, IPv4, and 100BaseT Ethernet
- Why is CRTP used?
- What is the major advantage of WebRTC?

# End of Applications