Selecting Standards That Will Be Implemented

Henning Schulzrinne
Dept. of Computer Science
Columbia University
New York, New York
schulzrinne@cs.columbia.edu

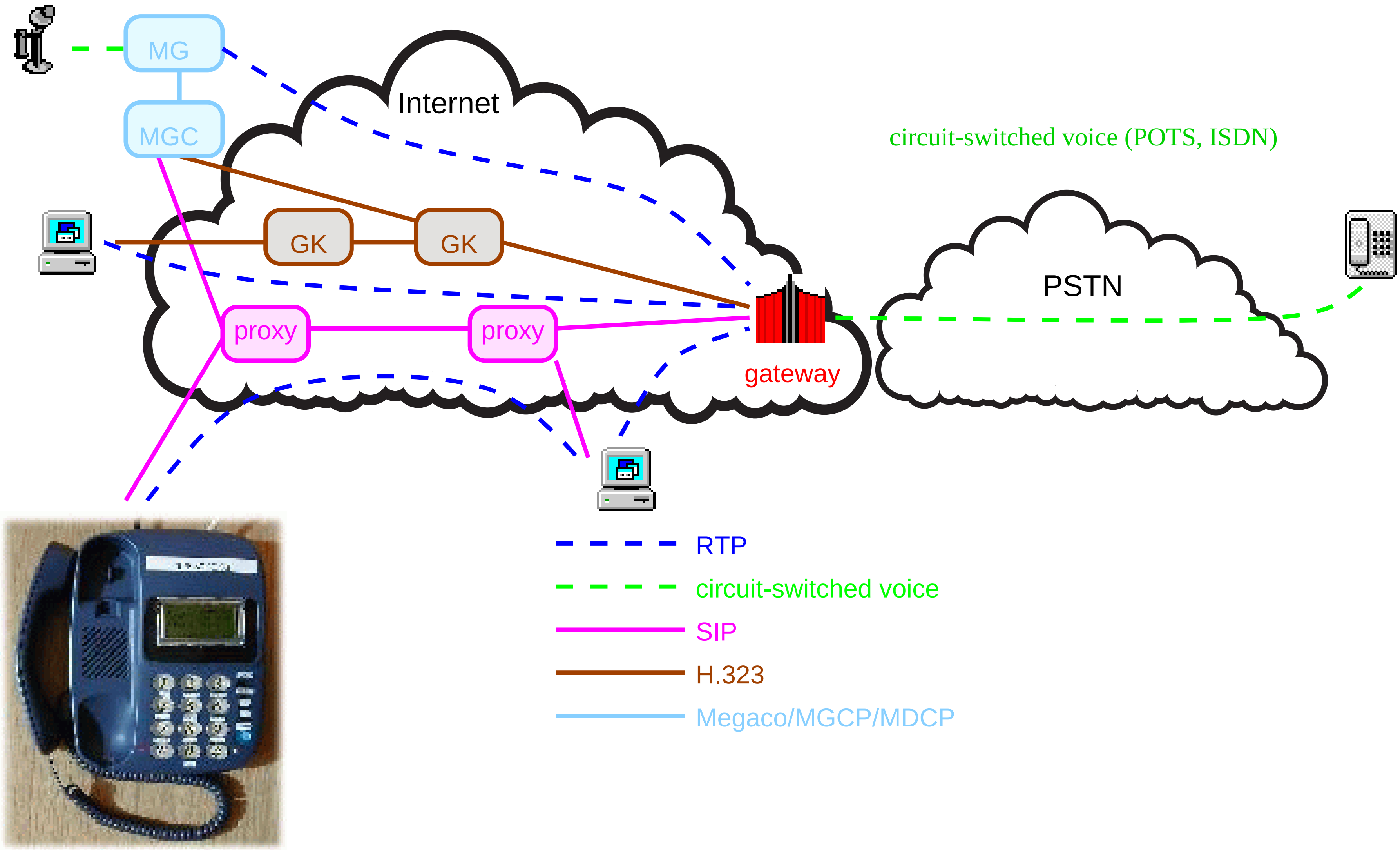
ICM – Carrier Class IP Telephony

January 19, 2000

Overview

- Architectures: peer vs. master/slave
- Master/slave: MGCP and Megaco
- Peer-to-peer
  - H.323
  - SIP
- services beyond signaling
- the standards process
- security issues

Architecture



Peer-to-Peer Architecture

- “IP telephones”, gateways, PCs with software = IP hosts
- *may* use servers (H.323 gatekeepers, SIP proxy servers)
- end system fully state-aware
- protocols for call setup: H.323 or SIP
- more flexible user interface

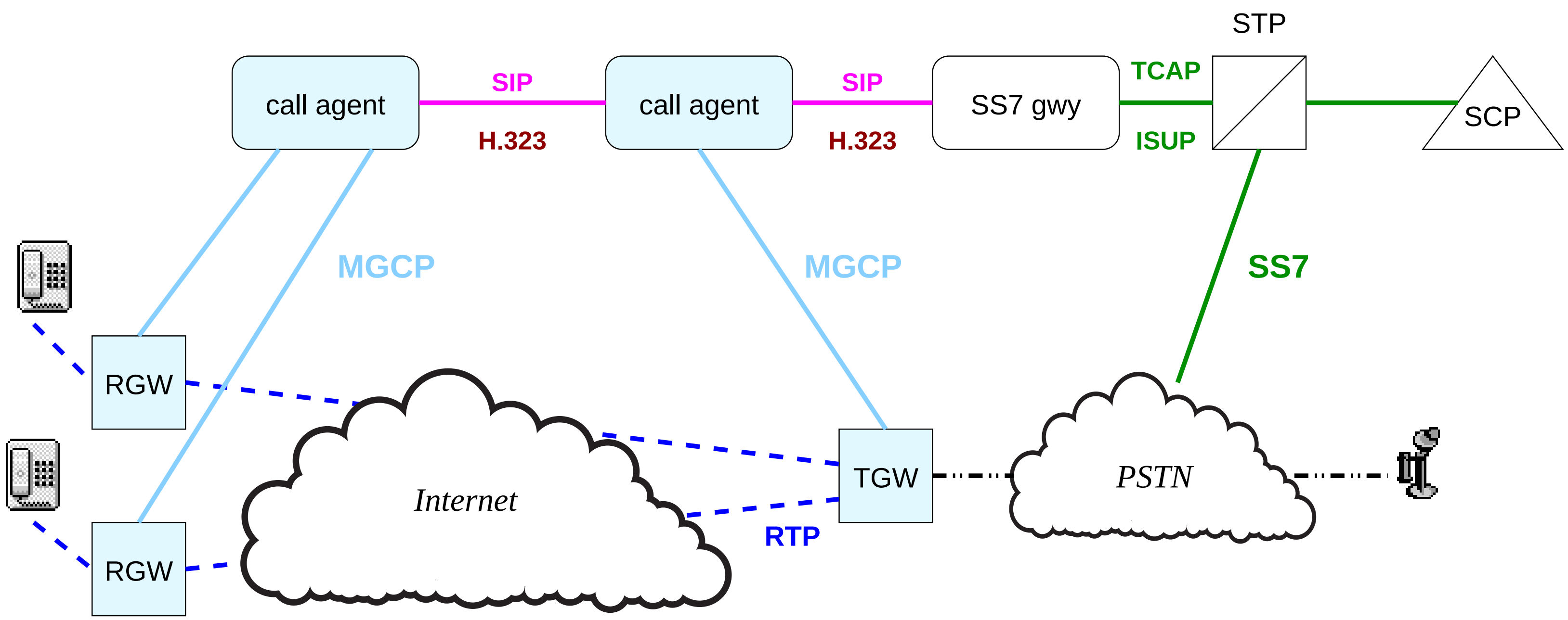
Implementing Services

	end system	server
caller id	x	–
call forwarding, follow me	x	x
three-way calling	x	–
distinctive ringing	x	–
69	x	?
no solicitation	x	x
do not disturb	x	x
call curfew	?	x

Master-Slave Architecture

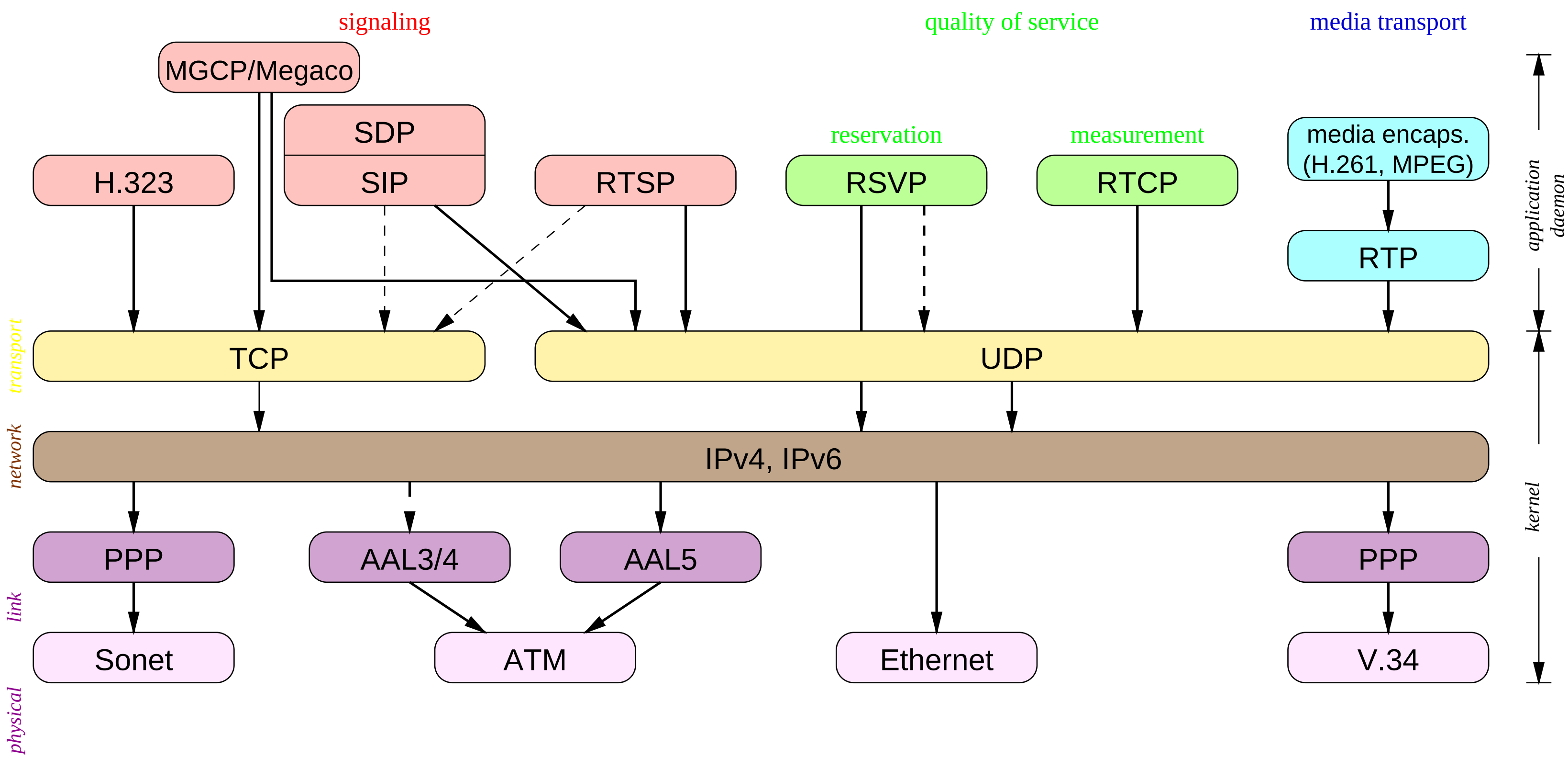
- master-slave: MGC controls one or more gateways
- allows splitting of signaling and media functionality
- “please send audio from circuit 42 to 10.1.2.3”
- uses MGCP (finished) or Megaco/H.248 (evolving)
- gateway can be residential
- basis of PacketCable NCS (network control system) architecture
- service creation similar to digital PBX or switch
- $\longrightarrow$ can charge for caller id, call waiting

MGCP Architecture



- for all but small system, need peer-to-peer!
- MGCP system can call SIP or H.323 end system
- all use RTP to transfer data

IETF Protocol Stack



IETF Architecture

Call setup, registration: SIP, MGCP/Megaco

Data transport: RTP, with RTCP for monitoring

Voice mail: RTSP

QOS resource reservation: RSVP, YESSIR, . . .

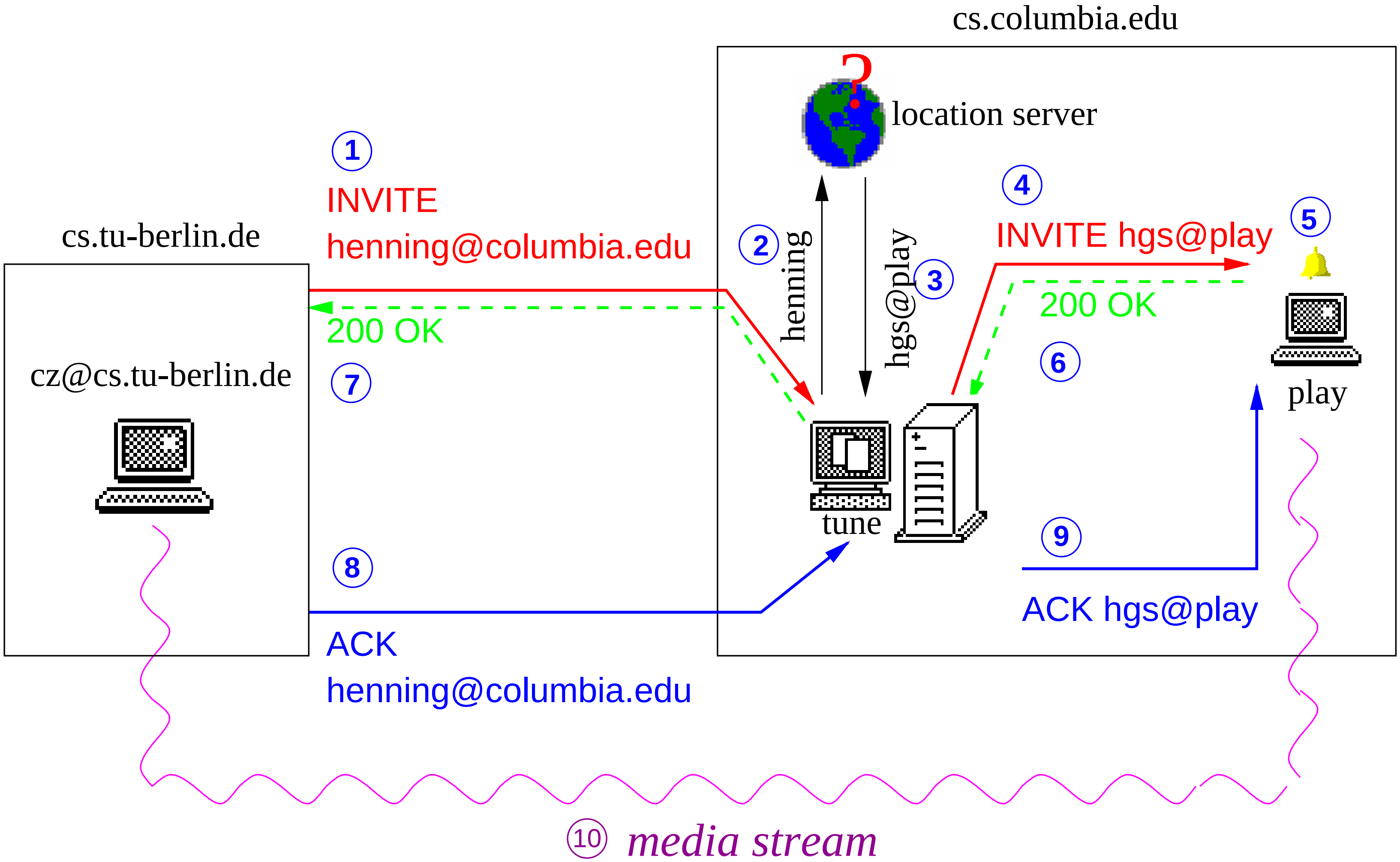
Locating gateways: TRIP

SIP 101

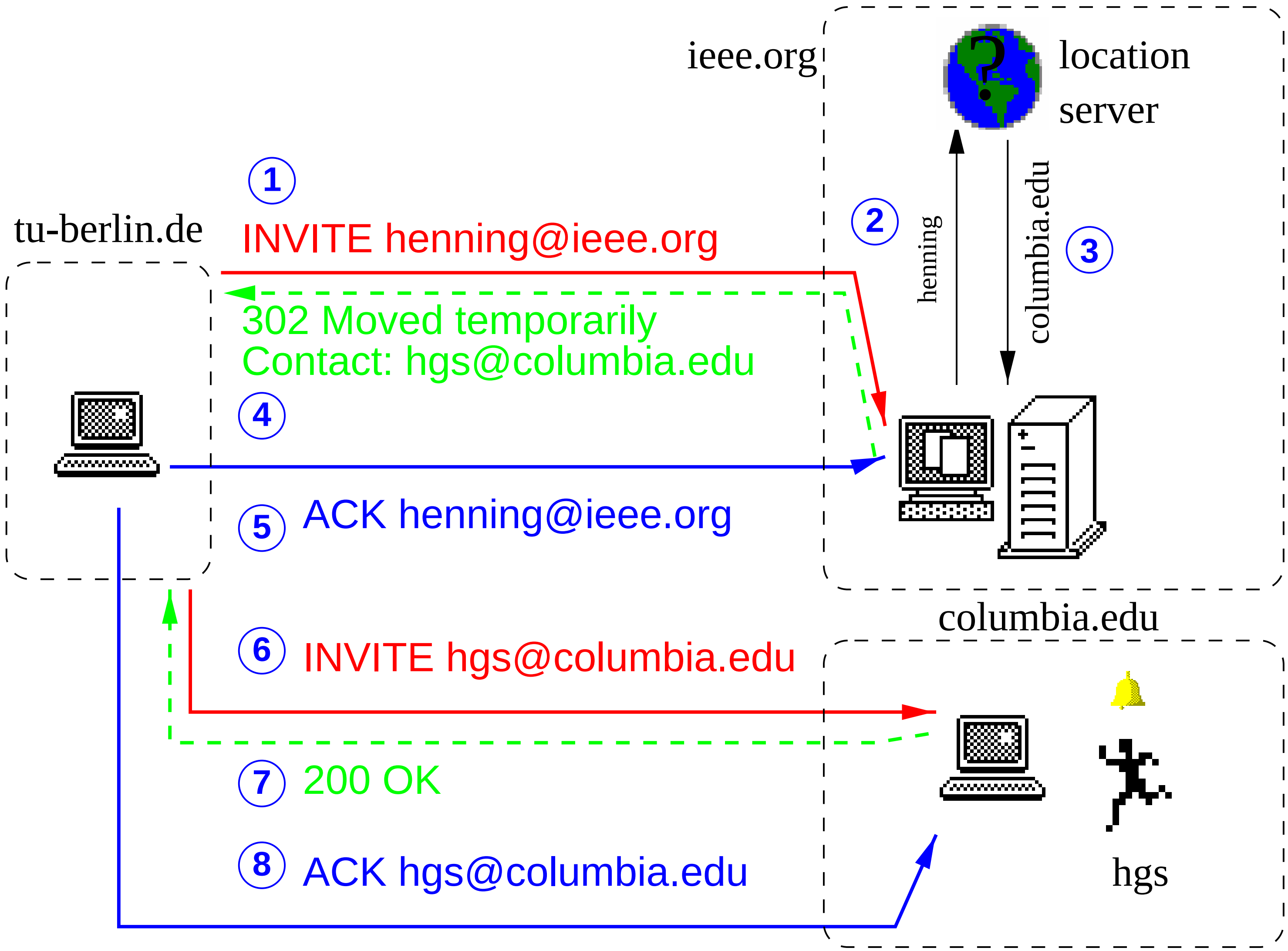
- SIP = signaling protocol for establishing sessions/calls/conferences/...
- session = audio, video, game, chat, ... – described by SDP carried in SIP message

1. called server may map name to *user@host*
2. callee accepts, rejects, forward ($\rightarrow$ new address)
3. if new address, go to step 1
4. if accept, caller confirms
5. ... conversation ...
6. caller or callee sends BYE

SIP Operation in Proxy Mode



SIP Operation in Redirect Mode



SIP Advanced Features

- operation over UDP or TCP
- multicast invitations ➠ basic ACD
- “interactive web response” (IWR)
- UA $\leftrightarrow$ proxy = proxy/redirect $\leftrightarrow$ proxy/redirect
- stateless proxies: self-routing responses
- forking proxies: call several in sequence and/or parallel
- security: basic (password), digest (challenge/response), PGP

More SIP Internet Telephony Services

- camp-on without holding a line
- short message service (“instant messaging”)
- schedule call into the future
- call with expiration date
- add/remove parties to/from call ➠ mesh
- “buddy lists”

Internet Telephony – as Part of Internet

- email address = SIP address
- SIP URLs in web pages
- forward to email, web page, chat session, . . .
- include web page in invitation response (“web IVR”)
- RTSP: choose your own music-on-hold
- include vCard, photo URL in invitation

SIP Status and Issues

- standard since early 1999
- three bake-offs in 1999 for interoperability testing, about 30 companies attending
- work in progress:
  - interaction with RSVP
  - caller preferences (“no mobile phones, please”)
  - call control
  - interoperation with ISUP
- issue: SDP expressiveness

SIP Bake-Off Participants

3Com	dynamicsoft	Mitel
8x8	Ellemtel	Netspeak
Agilent	Ericsson	Nortel
Alcatel	Facet	Nuera
Broadsoft	Helsinki Univ.	OZ.com
British Telecom	Hewlett-Packard	Pingtel
Catapult	Indigo	Radcom
Cisco	IPcell	Telogy
Columbia University	Lucent	Vovida
Dialogic	MCI Worldcom	VTEL
	Mediatrix	

H.323 – Components

H.225.0: call control, RAS→GK: "may I?", user location; RTP/RTCP

H.235: security for H.323 terminals

H.245: capabilities exchange, indications, notifications

H.246: interoperability with PSTN

H.332: large group conferences

H.450: supplementary services

H.246: interworking between H.323 and other H.xxx standards

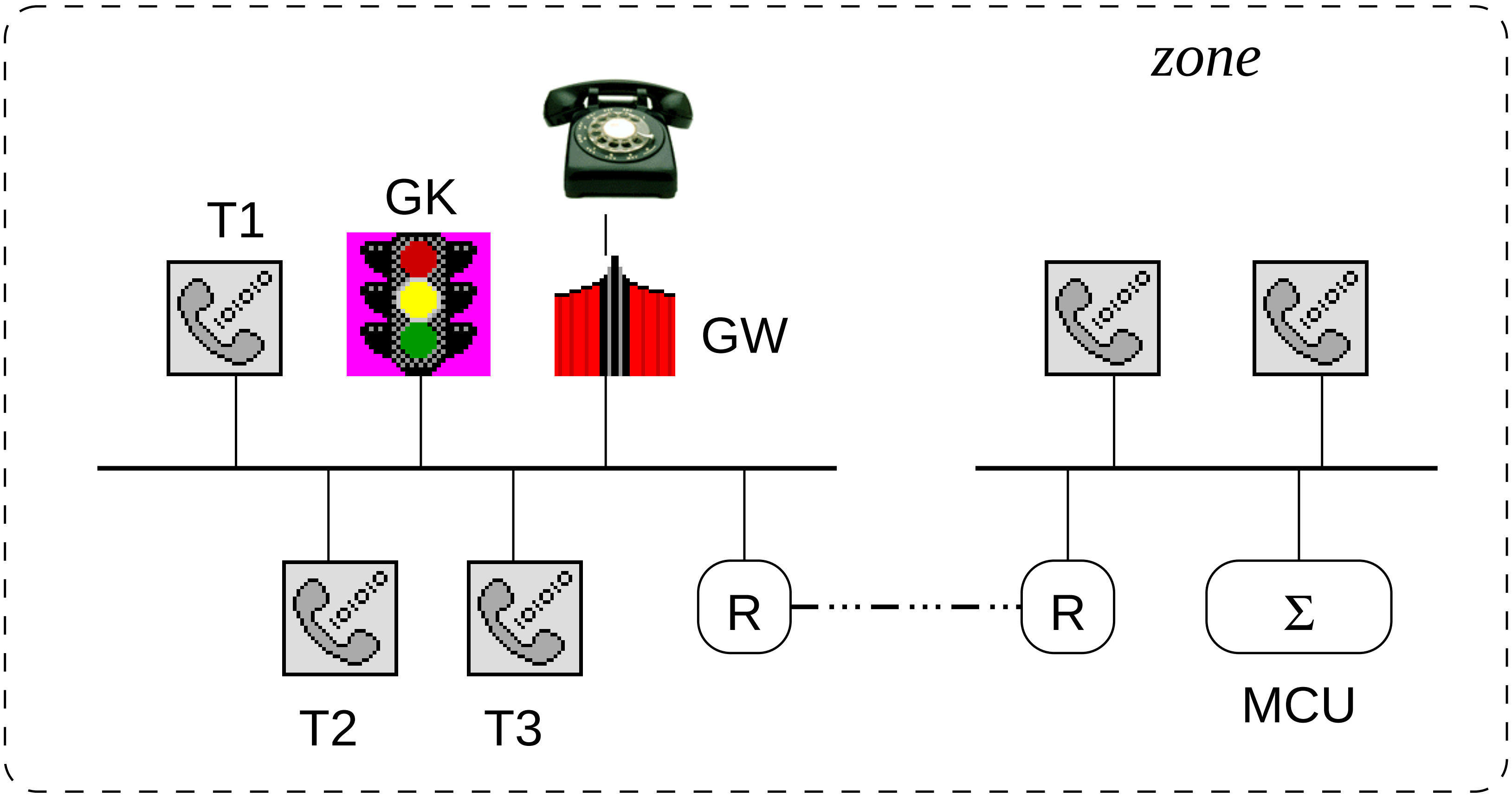
Q.931: call setup = ISDN, similar to Q.2931 (ATM)

Q.932: supplementary services

H.323

- derived from H.320 (ISDN multimedia)
- mostly ASN.1 (PER) based, but also Q.931
- several versions, with support for all needed
- signaling TCP-based, except for H.323v3

H.323 Zones



H.323 gatekeeper

- controls sessions
- performs user location and registration
- admission control
- reroutes signaling
- processes RAS (registration, admission, status) from H.323 terminals

H.323 Phases

Initialization: register with GK

GK admission: obtain permission; GK resolves address

Call signaling: signaling connection to peer
call initiation and completion/rejection

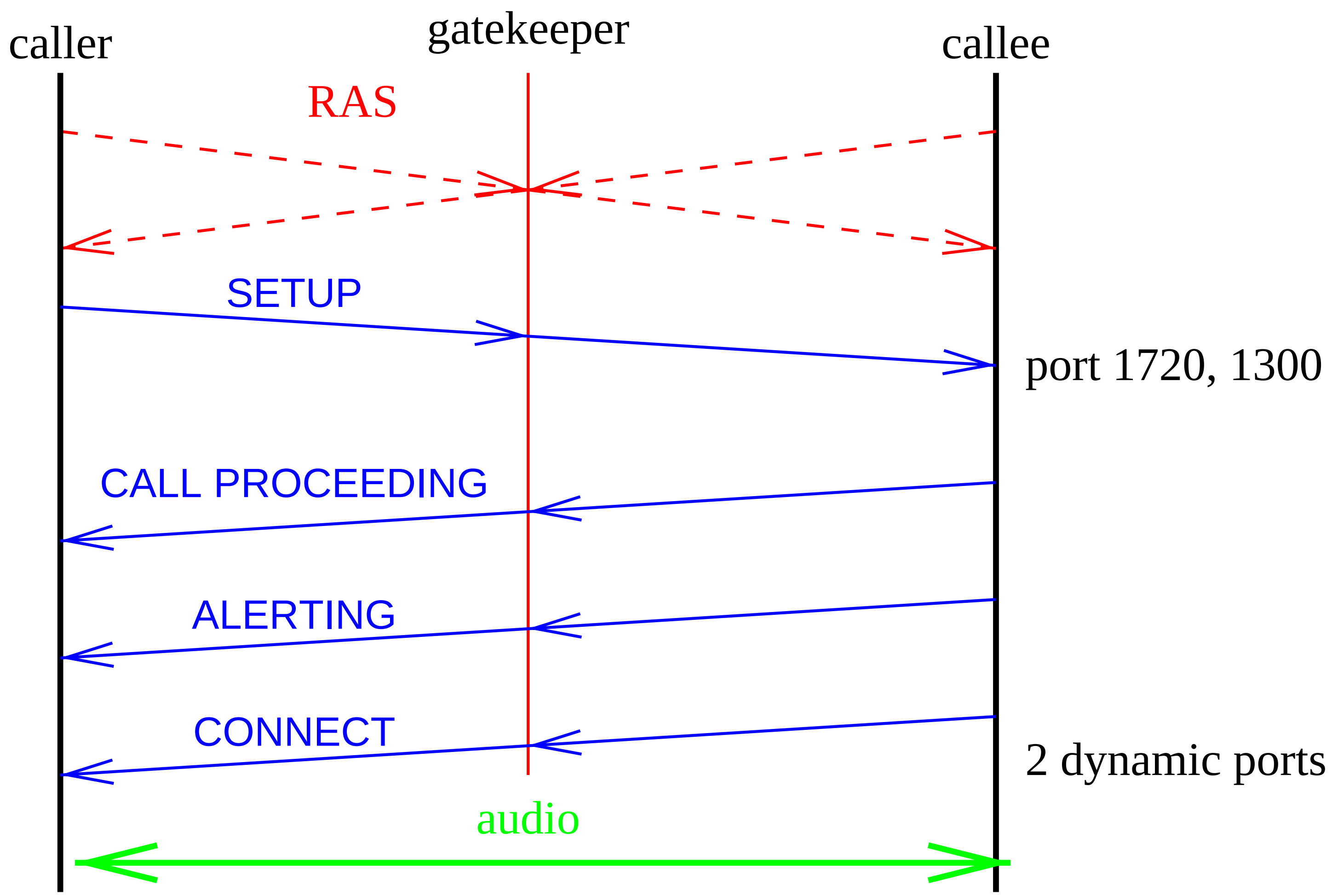
Negotiation/configuration: negotiate roles during call
capability exchange; determine mode of operation

Media exchange: configure and open logical channels
transmit and receive data streams

Re-negotiation: change members, parameters, media, . . .

Shutdown: terminate the call/conference
deregister user on log-off

H.323v3 call setup



H.323 problems

- already at version 4, most support version 2
- very complex (200+ pages; 65 pages for call forwarding!)
- no multicast signaling
- limited multicast conferences (➠ MCUs)
- call = TCP connection $\leftrightarrow$ mobility, reliability
- but: better capability negotiation (H.245)
- no media servers
- agile ports ➠ firewalls difficult

SIP – H.323 comparison

	H.323	SIP
Architecture	stack	element
Conference control	yes	no
Protocol	mostly TCP	mostly UDP
Encoding	ASN.1, Q.931	HTTPish
Emphasis	telephony	multimedia, multicast
Address	flat alias, E.164	SIP, E.164 URLs

Both SIP and H.323 are evolving: SIP additions, H.323v2 implements some SIP features, v3 to be decided.

H.323 vs. SIP Carrier Issues

- most hardware currently speaks H.323
- longer term: bilingual, can coexist within same system
- interworking specification in progress, demonstrated SIP phone call NetMeeting

Primary Standards Organizations

IETF: open process, Internet-focused:

sip	SIP extensions (call control, caller preferences, ...)
iptel	CPL, TRIP
avt	RTP
enum	E.164 $\xrightarrow{DNS}$ IP
megaco	MEGACO/H.248
mmusic	SAP, SDP

ITU SG.16: H.323 and related work

Secondary (Standards) Organizations

Softswitch Consortium: MGCP, SIP, RTP, RTSP; nominally, H.323

IMTC: iNow!, aHit! – interoperability "clean up"

ETSI Tiphon: mostly European, "glue" documents, interoperability, architecture, . . .

Security Threats

Theft of service: primarily applicable for resource reservation protocols

Denial of service: repeated calls, bogus registrations to fill up database, bogus termination request, . . .

Disclosure of sensitive data: call path, user identity

Impersonation of identity: calls, registration

Security Protections

- lower-layer: SSL/TLS, IPsec – but needs shared secret or certificate
- TLS $\longrightarrow$ significant call setup delay
- unlike web server, every household needs certificate!
- some protection through randomness of call identifier (SIP), request sequence number or use of TCP connections
- SIP: password, digest (challenge/response) with shared secret, PGP for certificate-based security
- H.323: own security or TLS/IPsec (H.235)

Conclusion

- peer-to-peer always needed, master-slave for local use
- proliferation of standards bodies, but two do “real” work
- security issues require more attention

For more information...

SIP: http://www.cs.columbia.edu/sip

RTP: http://www.cs.columbia.edu/~hgs/rtp

Papers: http://www.cs.columbia.edu/IRT