Kommunikationssysteme (KSy) - Block 5

Voice over IP (VoIP) Part 2

Dr. Andreas Steffen

H.323 Network Components

- Terminals, gatekeepers, gateways, multipoint control units

H.323 Gateway

- Gateway to PSTN, protocol translation, audio/video transcoding

H.323 Gatekeepers

- H.323 zones
- Automatic gatekeeper discovery
- Endpoint registration, unregistration, location and admission to network
- Summary of gatekeeper functionalities

H.323 Call Setup and Control

- Q.931 call signalling channel (gatekeeper-routed and direct call setup)
- H.245 control channel (gatekeeper-routed and direct control)
- H.245 capabilities exchange

Channel Multiplexing

- H.225.0 channel multiplexing
- Transport of logical channels over IP-based networks using UDP and TCP

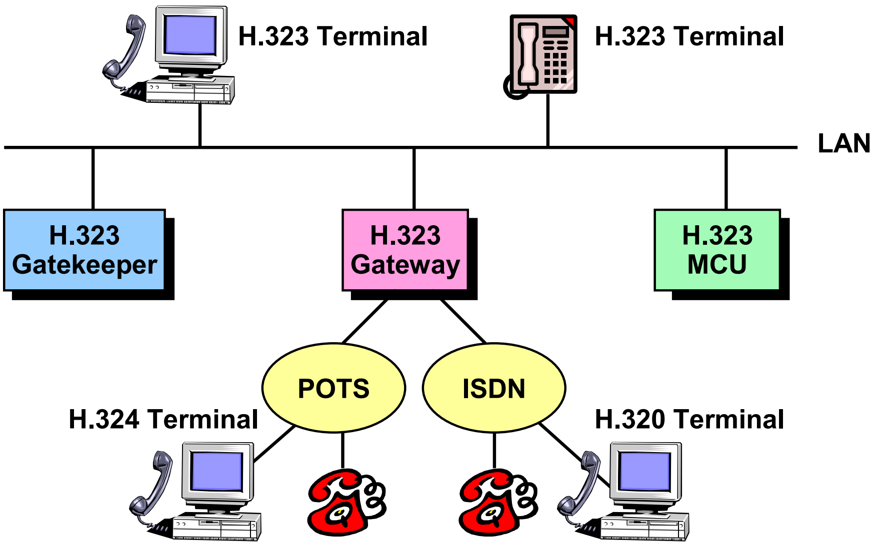
Multipoint Conferences

- Multipoint control and multipoint processor functions for multipoint conferencing
- Centralized and decentralized multipoint conferences

Session Initiation Protocol (SIP)

- SIP uniform resource locators
- SIP Invitation using a SIP proxy server
- Example of an INVITE request

H.323 Network Components



H.323 Terminals

- H.323 Terminals are the **client endpoints** on the LAN that provide real-time, two-way communications. They can be realized either as SW-Clients running on a PC or workstation or as dedicated HW-devices like e.g. IP-phones. All terminals must support voice communications; video and data are optional.

H.323 Gatekeeper

- A Gatekeeper is the most important component of an H.323 enabled network. It acts as the central point of all calls within its **zone** and provides call control services to **registered** endpoints. Gatekeepers perform two important call control functions. The first is **address translation** from LAN aliases or phone numbers for terminals and gateways to IP addresses. The second function is **bandwidth management**.

H.323 Gateway

- A Gateway is an optional element in an H.323 conference. Gateways provide many services, the most common being a translation function between H.323 endpoints and other terminal types. In addition, the gateway also translates between audio and video codecs and preforms call setup and clearing on both the LAN side and the PSTN side.

H.323 Multipoint Control Unit (MCU)

- The Multipoint Control Unit supports conferences between three or more endpoints. Under H.323 an MCU consists of a **Multipoint Controller** (**MC**), which is required, and zero or more **Multipoint Processors** (**MP**). The MC handles negotiations between all terminals and controls the conference resources, whereas the MP mixes, switches and processes audio, video, and/or data.

Source: „A Primer on the H.323 Series Standard“, 1998, DataBeam Corporation

H.323 Gateways

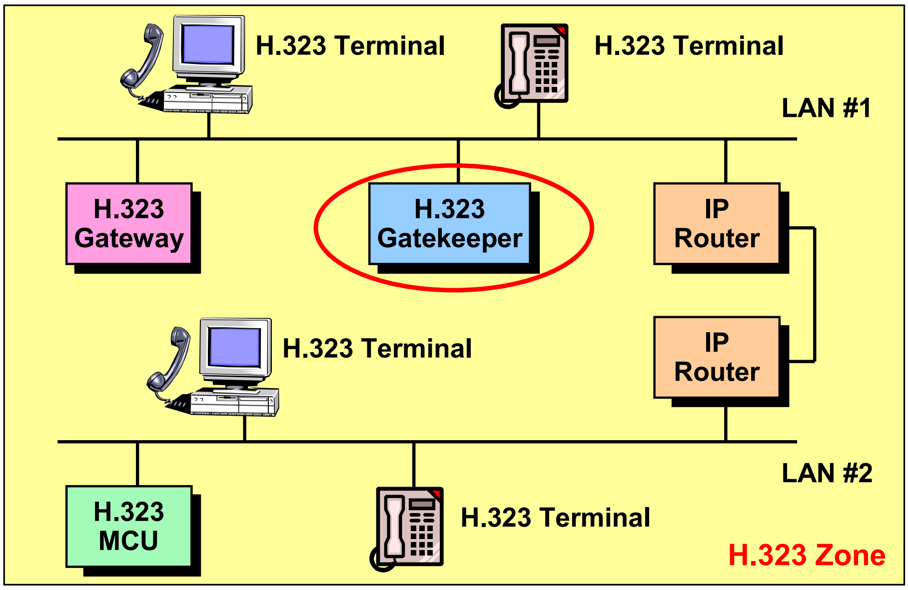
H.323 / PSTN Gateway Functionality

Zürcher Hochschule Winterthur

- Physical Interface LAN ←→ PSTN
  - POTS (analog line)
  - ISDN (digital line)
- Call Setup
  - Setup and release of calls on both the LAN and the PSTN side.
- Translation of Transmission Multiplex Formats
  - H.225.0 to H.221 / H.223
- Translation of System Control Protocols
  - H.245 to H.242
- Audio / Video Transcoding
  - Translation among audio codecs, conversion to analog voice
  - Translation among video codecs (if terminals do not support negotiation)

H.323 Gatekeepers

H.323 Zone managed by a Gatekeeper

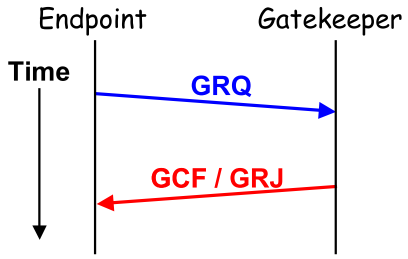


H.323 Zones

- The collection of all Terminals, Gateways and Multipoint Control Units managed by a single gatekeeper is known as an H.323 Zone. A zone can cover several IP subnets that are separated by IP-routers.
- A gatekeeper usually keeps a list of neighbouring zones, so that a call setup request to a H.323 client belonging to a distant zone can be routed by gatekeepers along the way on a hop-by-hop basis.

Registration, Admission and Status (RAS)
Automatic Gatekeeper Discovery

Zürcher Hochschule Winterthur



Who is my Gatekeeper ?

GRQ Gatekeeper Request

I can be your Gatekeeper !

GCF Gatekeeper Confirmation

I don't want to be your Gatekeeper !

GRJ Gatekeeper Reject

Gatekeeper Discovery IP Multicast Address	**224.0.1.41**
Gatekeeper Discovery UDP Port	**1718**

Registration, Admission and Status (RAS) Protocol

- The RAS protocol is defined in the ITU-T H.225.0 recommendation. The protocol is used between H.323 endpoints and the gatekeeper of the H.323 zone they are assigned to.

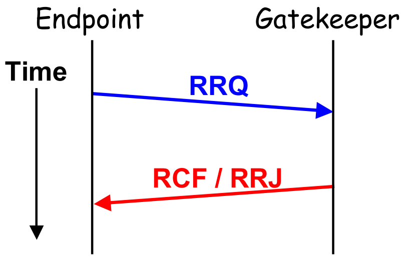
Automatic Gatekeeper Discovery

- If an H.323 endpoint does not know its gatekeeper, then it can send a **Gatekeeper Request** (**GRQ**). This is a UDP datagram addressed to the well-known destination port 1718 and transmitted in the form of an **IP multicast** with the multicast group address 224.0.1.41.
- One or several gatekeepers can answer the request with either a positive **Gatekeeper Confirmation** (**GCF**) message or a negative **Gatekeeper Reject** (**GRJ**) message. A reject message contains the reason for the rejection and can optionally return information about alternative gatekeepers.

Source: ITU-T Recommendation H.225.0 „Call signalling protocols and media stream packetization for packet-base multimedia communication systems“, 02/98.

Registration, Admission and Status (RAS)
Endpoint Registration

Zürcher Hochschule Winterthur



RRQ Registration Request

- **callSignalAddress** IP address
- **terminalAlias**
  - terminal ID,
  - e-mail address,
  - phone number
- **timeToLive** in seconds
- **keepAlive** bit, set in refresh message

RCF Registration Confirmation

- **timeToLive** in seconds

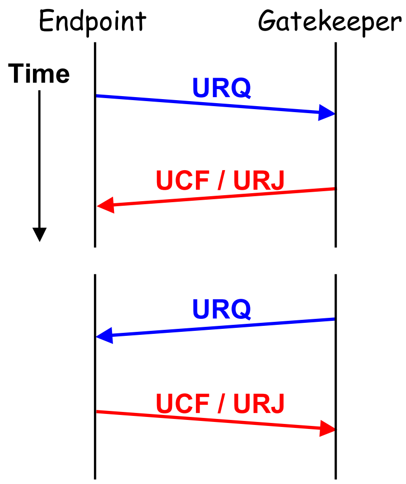
RRJ Registration Reject

Gatekeeper Registration and Status UDP Port	1719

Endpoint Registration

- When an H.323 endpoint is activated, then either its assigned gatekeeper is already preconfigured or the terminal tries to find it using the automatic gatekeeper discovery procedure. As a next step the terminal registers with its gatekeeper by sending a **Registration Request** (**RRQ**) message to the well-known Gatekeeper Registration and Status UDP Port 1719.
- Among the parameters sent in the RRQ message are the **callSignalAddress** field, which is the IP address of the H.323 client and one or several **terminalAlias** entries, that can be a terminal ID, a nick name, an e-mail address or the E.164 phone number of the H.323 user. The gatekeeper uses this information to build an entry into its user directory, linking aliases with corresponding IP destination addresses.
- An important parameter is the **timeToLive** field which defines the desired interval in seconds during which the registration shall be valid.
- Shortly before the expiration of the registration period the client can send a „light-weight“ RRQ message with the **keepAlive** bit set, in order to prolong the registration period.
- The gatekeeper responds to a registration request either with a **Registration Confirmation** (**RCF**) message, confirming or redefining the **timeToLive** parameter, or a **Registration Reject** (**RRJ**) message when the gatekeeper does not want to register the H.323 client.

Registration, Admission and Status (RAS)
Endpoint Unregistration



URQ Unregistration Request

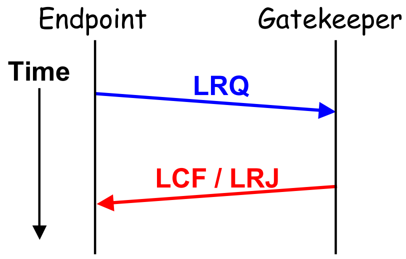
UCF Unregistration Confirmation

URJ Unregistration Reject

Endpoint Unregistration

- With an **Unregistration Request** (**URQ**) message either a H.323 client can revoke a previous registration with a gatekeeper or a gatekeeper can request a terminal to consider itself unregistered.
- The peer either answers with an **Unregistration Confirm** (**UCF**) message or an **Unregistration Reject** (**URJ**) message.

Registration, Admission and Status (RAS)
Endpoint Location



LRQ Location Request

alias address (ID, phone number) of an unknown endpoint

LCF Location Confirmation

callSignalAddress of located endpoint

LRJ Location Reject

endpoint not registered with gatekeeper (reply to unicast only)

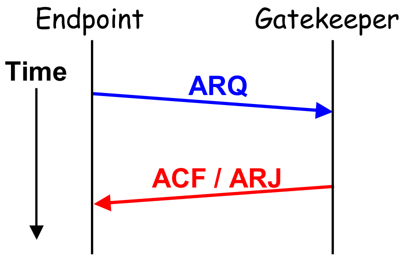
Gatekeeper Discovery IP Multicast Address	**224.0.1.41**
Gatekeeper Discovery UDP Port	**1718**

Endpoint Location

- When an endpoint knows the **alias address** (terminal ID, nick-name, e-mail address or phone number) of the peer it wants to call, then it can ask a gatekeeper for the corresponding IP-address. If the gatekeeper's IP address is known, then the endpoint sends a unicast UDP datagram containing a **Location Request** (**LRQ**) message to port 1718, otherwise the request is multicast with the multicast group address 224.0.1.41.
- If the gatekeeper finds an entry for the requested H.323 peer, it answers with the **Location Confirmation** (**LCF**) message containing the IP address in the **callSignalAddress** field. If the requested H.323 peer is not currently registered with the gatekeeper, it issues a **Location Reject** (**LRJ**) message.
- Gatekeepers queried by a multicast LRQ message do not reply with a Location Reject message when they cannot resolve the requested alias address. Thus a flooding of the IP network with superfluous datagrams can be avoided.

Endpoint Admission to Network

Zürcher Hochschule Winterthur



ARQ Admission Request

callModel
- **direct**
- **gatekeeperRouted**

bandWidth **requested AV bandwidth**

ACF Admission Confirmation

callModel, bandWidth

ARJ Admission Reject

Gatekeeper Registration and Status UDP Port	**1719**

Endpoint Admission to Network

- When an endpoint wants to make an H.323 call, it must first ask its gatekeeper for permission by sending an **Admission Request** (**ARQ**) message to UDP port 1719. The message contains among others the **callModel** parameter requesting either a **direct** call setup to the H.323 peer or a **gatekeeper-routed** call setup. With the **bandWidth** variable the client can reserve a desired audio/video bandwidth for the call.
- The gatekeeper either answers with an **Admission Confirmation** (**ACF**) message, optionally changing the **callModel** and/or decreasing the requested **bandWidth**. If the maximum of active calls has been reached or the available bandwidth does not allow for an additional call then an **Admission Reject** (**ARJ**) message is sent.

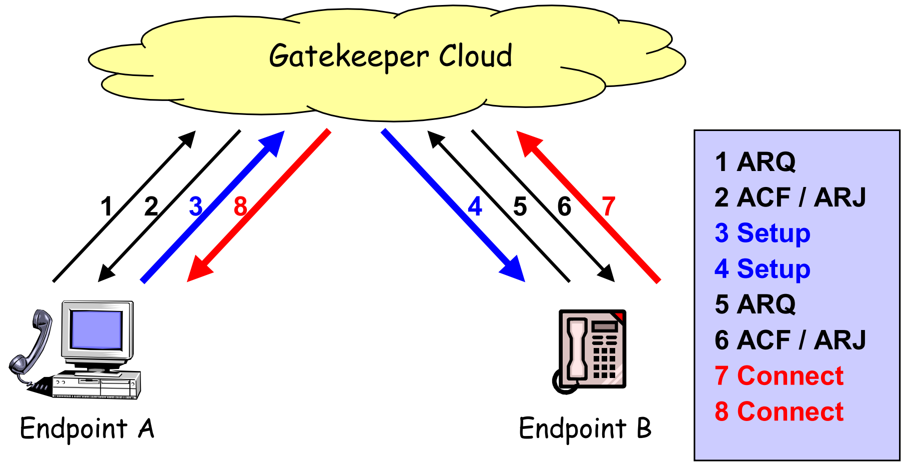
H.323 Gatekeeper Functionality

- Address Registration and Translation
  - RRQ/RCF/RRJ and LRQ/LCF/LRJ messages
  - Translation of alias adresses to transport Adresses
- Admission Control
  - ARQ/ACF/ARJ messages
  - Authorization of LAN access (call authorization, bandwidth)
- Bandwidth Control and Management
  - BRQ/BCF/BRJ messages
  - Dynamic change of requested and available bandwidth
- Call Authorization, Control and Management (optional)
  - Access restrictions, upper limits on simultaneous calls
- Zone Management
  - Gatekeepers provide above services for terminals, gateways and MCUs registered within their zone of control

Zürcher Hochschule Winterthur

H.323 Call Setup and Control

Call Signalling Channel (Q.931)
Gatekeeper-Routed Call Signalling



Gatekeeper / Endpoint Call Signalling TCP Port	**1720**

Q.931 Call Signalling Channel

- The Q.931 call signalling channel is defined in the ITU-T H.225.0 recommendation. It is carried over a reliable TCP connection using the well-known port 1720.

Admission Request by Calling Party

- The call setup starts by the calling party sending an ARQ message to the gatekeeper asking for a gatekeeper-routed call. The gatekeeper replies with a positive ACF message or aborts the call with an ARJ message.

Q.931 Setup Message

- The calling party now sends a Q.931 **Setup** message to TCP port 1720 of the gatekeeper. The gatekeeper cloud routes the message on a hop-by-hop basis to the calling party which receives the message on port 1720.

Admission Request by Called Party

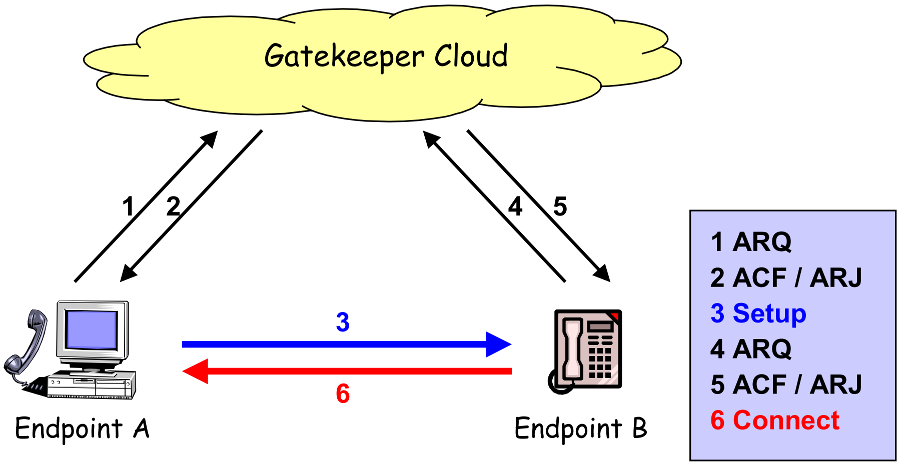
- Before the called party can answer the call, it must first ask its gatekeeper in turn whether sufficient bandwidth is available for the call by issuing an ARQ message. Only if it gets an ACF message in return it can accept the incoming call.

Q.931 Connect Message

- The Q.931 **Connect** message is now sent via the gatekeeper cloud back to the calling party. When the connect message is received, the bidirectional H.323 call has been successfully set up.

Call Signalling Channel (Q.931)
Direct Endpoint Call Signalling

Zürcher Hochschule Winterthur



Endpoint Call Signalling TCP Port	**1720**

Admission Request by Calling Party

- The call setup starts by the calling party sending an ARQ message to the gatekeeper asking for a direct call. The gatekeeper replies with a positive ACF message or aborts the call with an ARJ message.

Q.931 Setup Message

- The calling party now sends a Q.931 **Setup** message directly to TCP port 1720 of the called party.

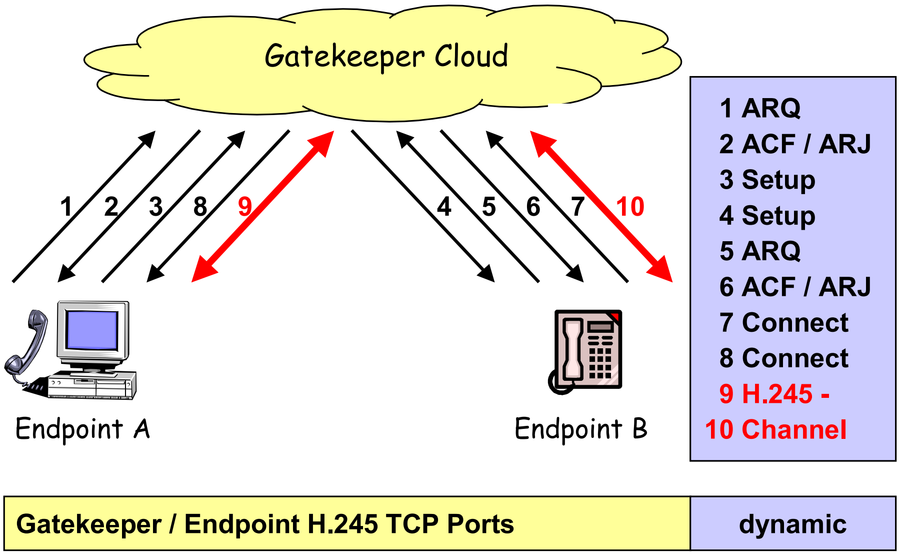
Admission Request by Called Party

- Before the called party can answer the call, it must first ask its gatekeeper in turn whether sufficient bandwidth is available for the call by issuing an ARQ message. Only if it gets an ACF message in return it can accept the incoming call.

Q.931 Connect Message

- The Q.931 **Connect** message is now sent directly back to the calling party establishing the bidirectional H.323 call between the two H.323 peers.

Control Channel (H.245)
Gatekeeper-Routed Control Channel



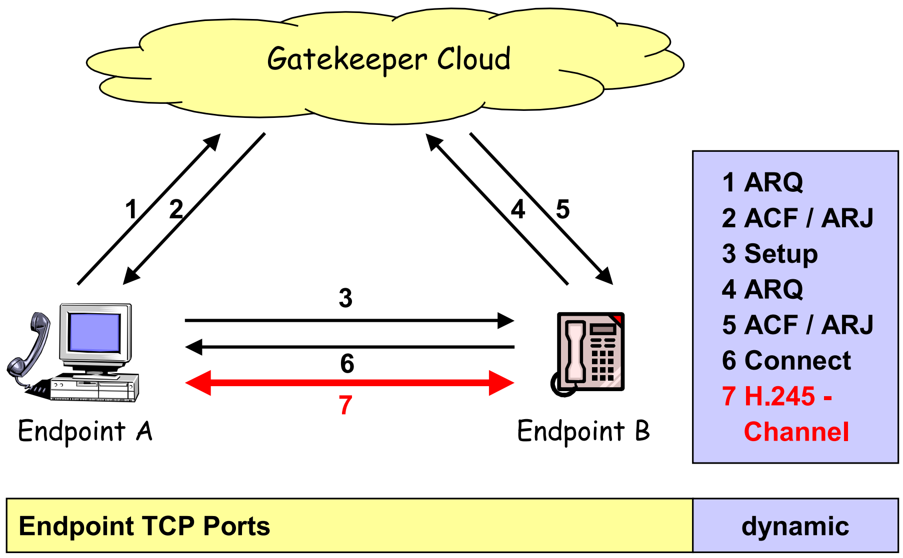
H.245 Control Channel

- As part of the Q.931 call setup, the TCP ports for the upcoming H.245 control channel are dynamically allocated. The destination TCP port number to be used in the H.245 connection is usually transmitted by the called party as part of the **Connect** message, but it could also be contained in any of the **CallProceeding**, **Progress** or **Alerting** messages or even in the **Setup** message sent by the calling party.
- The H.245 control channel is needed for the negotiation of the **common** video/audio and/or data capabilities that are supported by both endpoints.

Gatekeeper-Routed Control Channel

- In the case of a gatekeeper-routed control channel, the H.245 capabilites exchange is routed via the gatekeeper cloud, giving the gatekeeper(s) the possibility to listen in to the exchange.

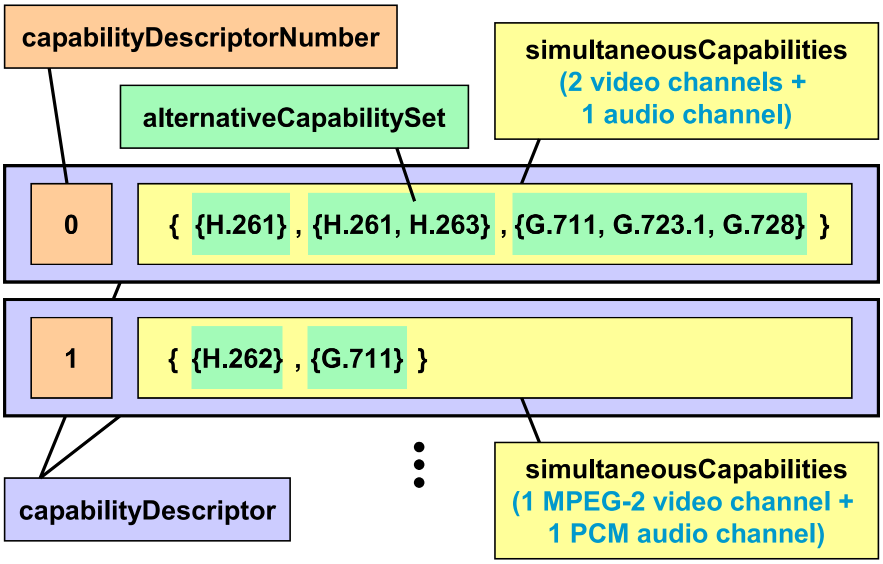
Control Channel (H.245)
Direct Control Channel Connection



Direct Control Channel Connection

- In this setup the H.245 capability exchange takes place directly between the two endpoints without being routed over the gatekeeper cloud.

H.245 Capabilities Exchange



alternativeCapabilitySet

- An alternativeCapabilitySet lists one or several alternative capabilities that are supported by an endpoint for a video, audio and/or data channel. E.g. the set **{H.261, H.263}** means that either the H.261 or the H.263 video codec could be used by the endpoint for a particular video channel. The set **{H.261}** means that only H.261 is supported.

simultaneousCapabilites

- During a multimedia call several capabilities are used simultaneously. In addition to an audio connection a user data application could be active at the same time. Our first example of a simultaneous capability

  { {H.261}, {H.261, H.263}, {G.711, G.723.1, G.728} }

  means that simultaneously two video channels and one audio channel must be supported. For the first video channel only the H.261 video codec can be used, for the second video channel the alternatives H.261 or H.263 exist, whereas for the audio channel any of the three codecs G.711, G.723.1 or G.728 can be chosen.

- In the second example

  { {H.262}, {G.711} }

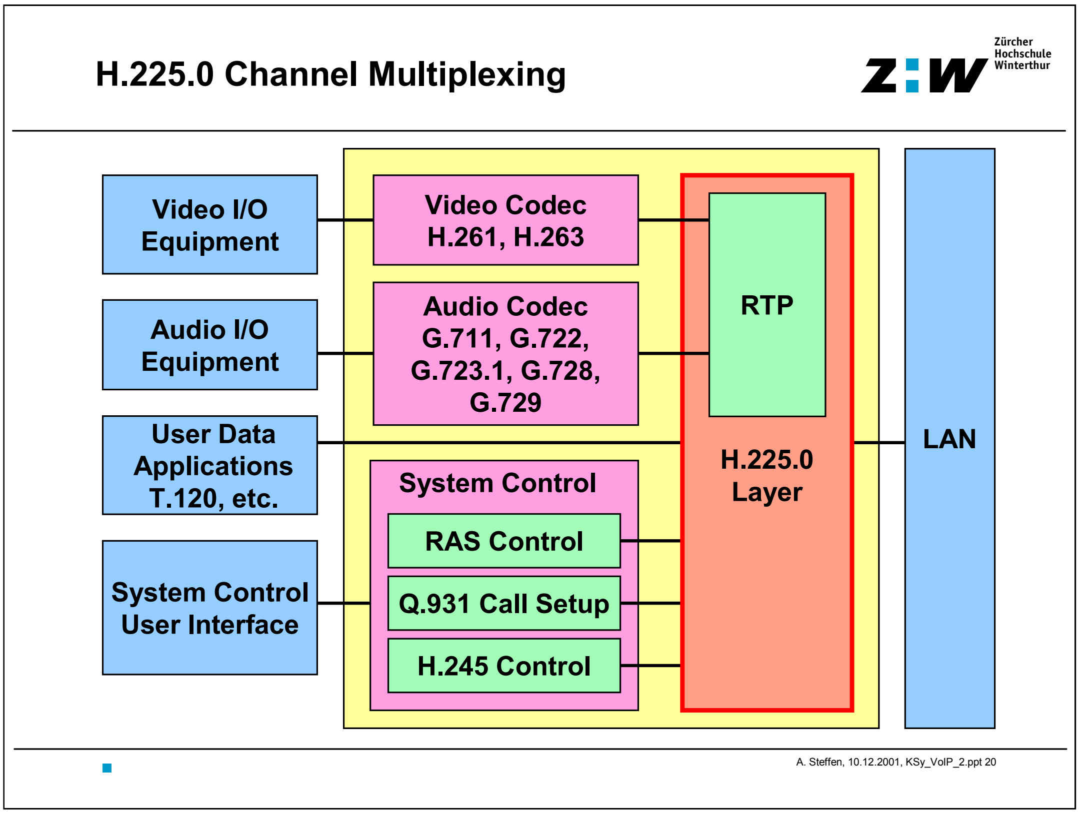
  a H.262 MPEG-2 video channel plus a G.711 PCM audio channel are required, with no alternatives for these codecs.

capabilityDescriptors

- An H.323 terminal can transmit an arbitrary number of capability descriptors identified by an increasing **capabilityDescriptorNumber**. Each capability descriptor describes one set of simultaneous capabilities.

- During the H.245 negotiation the two endpoints try to find a common capability descriptor containing the most powerful set of simultaneous capabilities with at least one match for each alternative capability set.

Channel Multiplexing



Channel Multiplexing

- All the H.323 channels defined in the previous slides must be transported over a LAN or WAN using the IP network layer. The various types of these connections and the relative order in which they are invoked, are described in detail by the ITU-T H.225.0 recommendation. The next slide will give a short overview on this topic.

Transport of Logical Channels
over IP-based Networks

Zürcher Hochschule Winterthur

	Standard	Transport Service
RAS Channel	H.225.0	UDP
Call Signalling Channel	Q.931	TCP
Control Channel	H.245	TCP
openLogicalChannel	H.245	
Audio Channels	G.7xx	UDP / RTP / RTCP
Video Channels	H.26x	UDP / RTP / RTCP
User Data Channels	T.120	TCP
closeLogicalChannel	H.245	

H.225.0 - RAS Channel

- This UDP-based channel is used by clients to find an associated gatekeeper and to register with it. Further it can be used to look up IP addresses of H.323 peers.
- Before a client can start a call, it must get admitted by the gatekeeper.

Q.931 - Call Signalling Channel

- A call is set up by the calling party using a reliable TCP connection to the well-known TCP destination port 1720.
- The TCP destination port for the H.245 control channel is negotiated dynamically.

H.245 - Control Channel

- The control channel is needed to find a set of common terminal capabilities. The exchange relies on a TCP connection.
- In a second phase, H.245 uses the **OpenLogicalChannel** command to negotiate the ports of the required audio, video and/or data channels and to open them:

  G.7xx - Audio Channels

  Audio is transported packed into unreliable UDP datagrams using the Real-time Transport Protocol (RTP). The Real-time Transport Control Protocol (RTCP) is used by the peer to give a feedback on the quality of the received audio stream.

  H.26x - Video Channels

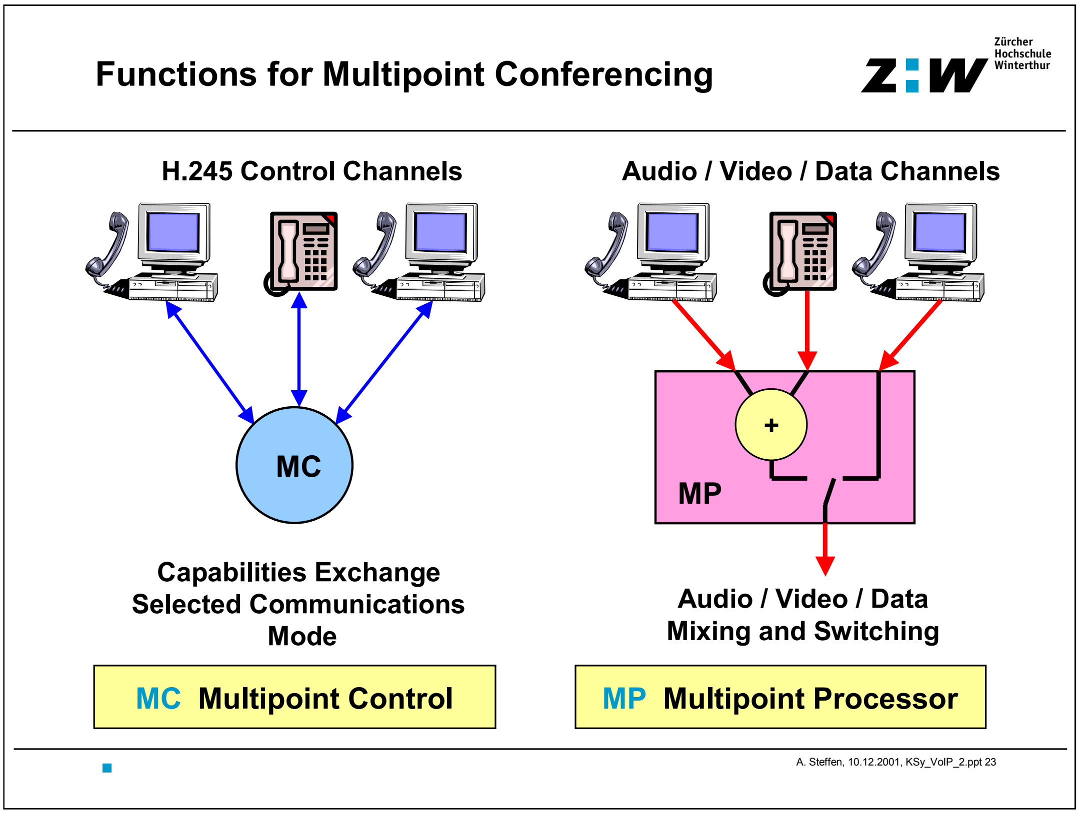
  Video is transported separately from audio over a different RTP/RTCP connection pair, also using the unreliable UDP transport layer.

  T.120 - User Data Channels

  User data for various applications are transported via a reliable TCP connection.

- When one of the H.323 peers terminates the call by transmitting a Q.931 **Release** message, then the associated H.245 control channel sends the required number of **CloseLogicalChannel** commands to close down all audio, video and data channels.

Multipoint Conferences



Logical Function Blocks for Multipoint Conferencing

- The Multipoint Control (MC) and the Multipoint processor (MP) are logical function blocks that can be located in a separate Multipoint Control Unit (MCU) or within a gatekeeper, a gateway or any H.323 terminal.

Multipoint Control

- The MC function block handles H.245 negotiations between all terminals to determine common capabilities for audio and video processing. The MC also controls conference resources by determining which, if any, of the audio and video streams will be multicast.

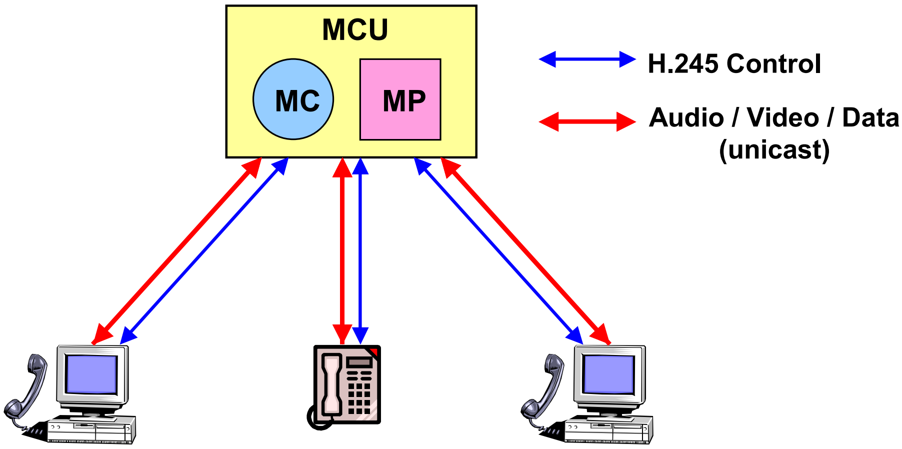
Multipoint Processor

- The MP function block mixes, switches and processes audio, video and/or data bits. The MP may also provide conversion between different codecs and bit rates and my use multicast to distribute processed video.

Source: „A Primer on the H.323 Series Standard“, 1998, DataBeam Corporation

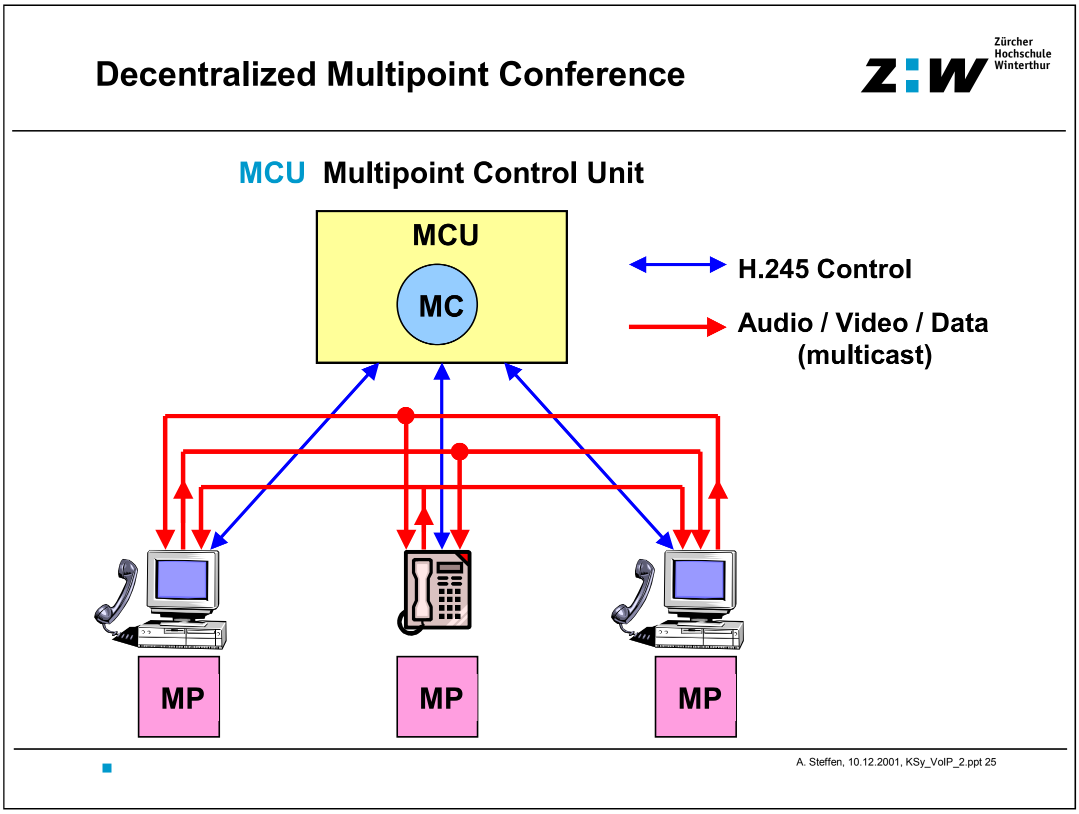
Centralized Multipoint Conference

MCU Multipoint Control Unit



Centralized Multipoint Conference

- Requires the existence of an MCU to facilitate a multipoint conference. All terminals send audio, video, data and control streams to the MCU in a point-to-point fashion. The MC centrally manages the conference using H.245 control functions that also define the capabilities for each terminal.
- The MP does the audio mixing, data distribution, and video switching / mixing functions typically performed in multipoint conferences and sends the resulting streams back to the participating terminals.
- A typical MCU that supports centralized multipoint conferences consists of an MC and an audio, video and/or data MP.



Decentralized Multipoint Conference

- Can make use of multicast technology. Participating H.323 terminals multicast audio and video to other participating terminals without sending the data to an MCU. Note that control of multipoint data is still centrally processed by the MCU, and H.245 Control Channel information is still transmitted in a point-to-point mode to an MC.
- Receiving terminals are responsible for processing the multiple incoming audio and video streams. Terminals use H.245 control channels to indicate to an MC how many simultaneous video and audio streams they can decode. The number of simultaneous capabilities of one terminal does not limit the number of video or audio streams which are multicast in a conference. The MP can also provide video selection and audio mixing in a decentralized multipoint conference.

Session Initiation Protocol (SIP)
IETF RFC 2543

SIP - Uniform Resource Locators

- **Examples of SIP URLs**

```
sip:andreas.steffen@zhwin.ch
sip:andreas.steffen@strongsec.com;transport=tcp
sip:sna@pcsn.zhwin.ch:3013
sip:sna@160.85.129.35:3013
sip:+41-76-340-2556@sipgate.diax.ch;user=phone
sip:434@gateway.zhwin.ch;user=phone
sip:zhwin.ch;method=REGISTER
```

- **Defaults**

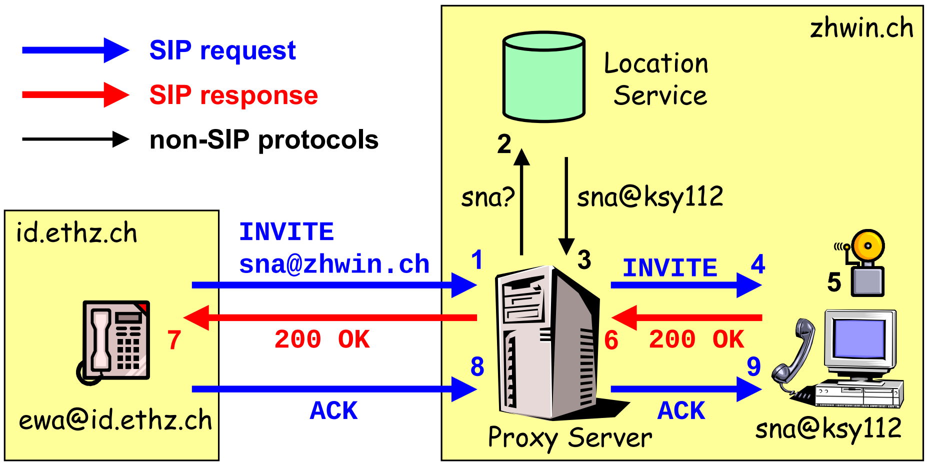
```
:5060            (destination port)
transport=udp    (transport parameter)
user=ip          (user parameter)
method=INVITE    (SIP method)
```


SIP Uniform Resource Locators

- A **sip:** URL is constructed in a similar way as a **http:** or **mailto:** URL.
- SIP URLs can have additional parameters that are appended by using **";"** as a separator.
- For each particular parameter not present, a predefined default value is assumed.
- SIP URLs can be embedded e.g. into an HTML page or an e-mail message. Clicking onto the link will automatically start a SIP call.

Source: RFC 2543 „SIP: Session Initiation Protocol", IETF, March 1999, pp. 20-24

SIP Invitation
using a SIP Proxy Server



Step 1

- The user **ewa@id.ethz.ch** wants to call **sna@zhwin.ch**. She send a SIP **INVITE** request to the proxy server **sip.zhwin.ch** responsible for the domain **zhwin.ch**.

Step 2

- The proxy server makes use of a location service (this can be an LDAP server or some alternative mechanism) which and queries the present location of user **sna**.

Step 3

- The location service returns as a result for the current location of user **sna** the SIP URL **sna@ksy112**. This is a local address within the **zhwin.ch** domain.

Step 4

- The proxy server now forwards the SIP **INVITE** message to the host **ksy112**.

Step 5

- Since the user **sna** is currently logged in, a bell is ringed, signalling the arrival of an incoming call.

Step 6

- As soon as the user **sna** accepts the call, a SIP response with the code **200 OK** signifying a successful request is sent back to the proxy server.

Step 7

- The SIP response is forwarded the calling party **ewa@id.ethz.ch**.

Step 8

- The calling party sends a SIP **ACK** message to the proxy server.

Step 9

- The proxy server forwards the SIP **ACK** message to the called party.

SIP - Example of an INVITE Request

```
INVITE sip:sna@zhwin.ch SIP/2.0
Via: SIP/2.0/UDP sip.zhwin.ch
From: Ewa Steffen <sip:ewa@id.ethz.ch>
To: Andreas Steffen <sip:sna@zhwin.ch>
Call-ID: 3298420296@delphi.ethz.ch
Cseq: 1 INVITE
Subject: Organisation Fondueplausch
Content-Type: application/sdp
Content-Length: ...
```

```
v=0
o=ewa 53655765 2353687637 IN IP4 129.132.35.30
c=IN IP4 sip.zhwin.ch
m=audio 3456 RTP/AVP 1 3 4
```

SDP: Session Description Protocol (RFC 2327)

SIP Header

- Similar to a MIME header.

Session Description Protocol

- v=* (version)
- o=* (owner/creator and session identifier)
- c=* (connection information)
- m=* (media type and transport address)

....

Capability Exchange and Multimedia Channels

- The capabilities of the calling terminal and the transport addresses of the requested audio, video and/or data channels are all sent as part of the initial SIP INVITE request.
- Due to this lightweight.protocol, a SIP session starts up much faster than an H.323 session.

Is SIP is going to replace H.323 over the next few years?