H.323 Addendum

A short summary of the differences between the various H.323 versions

H.323 History

- Version 1: "*visual telephone systems and equipment for LANs that provide a nonguaranteed quality of service (QoS)*"was accepted in October 1996.
  - Focus on multimedia communication in a LAN
  - No support for guaranteed QoS
- Version 2: "*packet-based multimedia communications systems*"was driven by the Voice-over-IP requirements and was accepted in January 1998.
- Version 3 was accepted in September 1999 and has minor incremental features (caller ID, etc.) over version 2.
- Version 4 was accepted in November 2000 and has significant improvements over version 3.

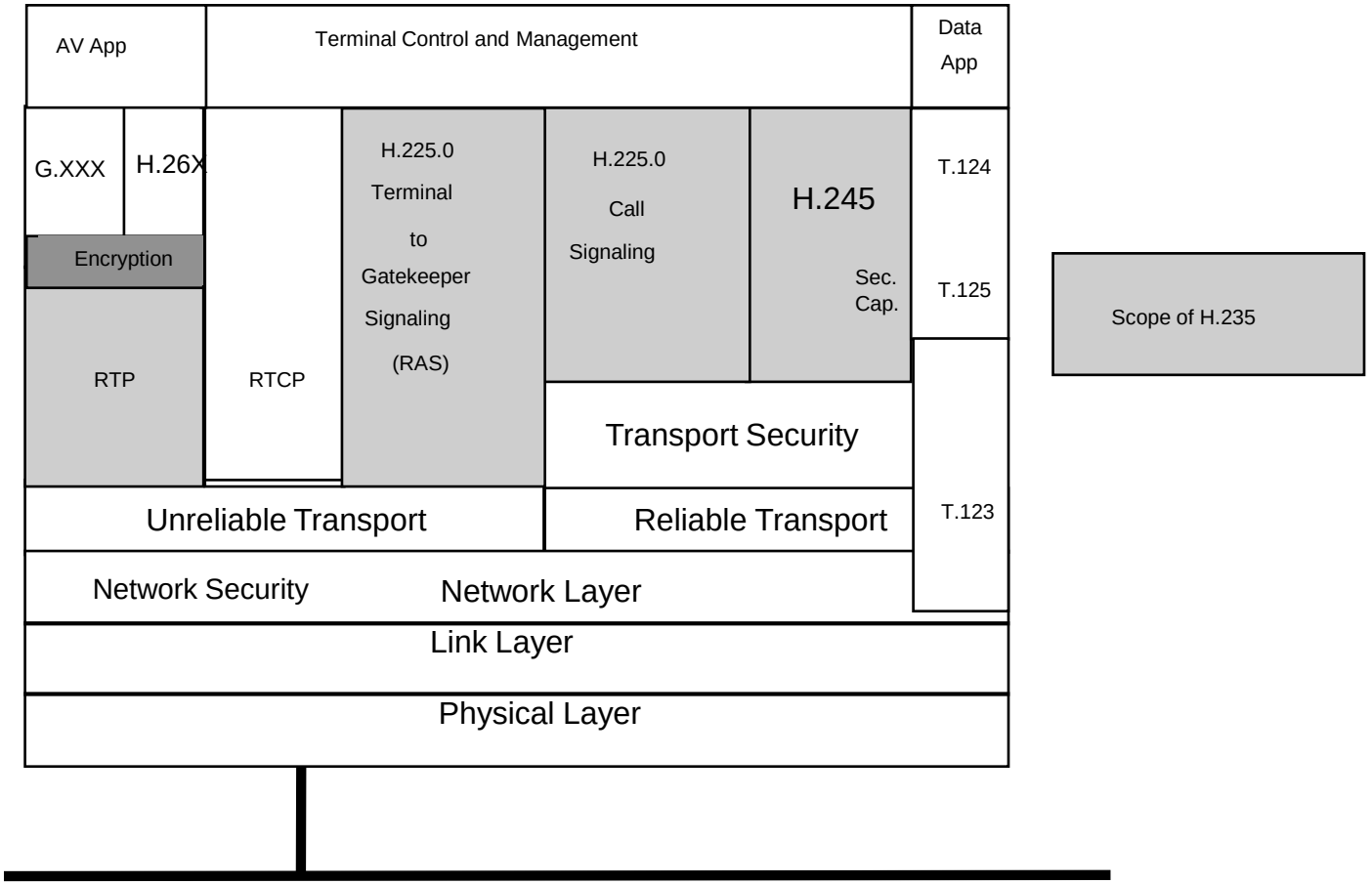
New Features in Version 2

- Version 2 (January 1998) adds:
  - New features within the existing protocols (H.225 and H.245)
  - New protocols
- Main features:
  - Security
  - Fast connect
  - Additional services
  - QoS enhancements
  - Gatekeeper enhancements
  - Additional media capabilities
  - Overlapped sending

H.323 V2 Security: H.235

- Services provided:
  - **Authentication**: verify the identity of the communication endpoints.
  - **Integrity**: verification that the data received on a network packet is indeed correct and has not been tampered with.
  - **Confidentiality**: protection of the data through encryption; if the conversation is being eavesdropped on, the content cannot be recovered.
  - **Non-Repudiation**: means of "proving" that someone was indeed in a conference (they cannot deny having taken part on it).

Scope of H.235



Types of Encryption

- Symmetric Encryption:
  - The same key is used both to encrypt and decrypt.
  - The key must be kept secret and must be communicated between the end nodes in some secure way.
  - Examples: DES, 3DES.
- Asymmetric Encryption:
  - Pair of keys: one public, one private.
  - Public key is freely given away, private key is kept secret.
  - What is encrypted by the public key can only be decrypted by the private key and vice-versa.
  - Example: RSA.

Uses of Asymmetric Encryption

- **Authentication and Non-Repudiation:**
  - Encrypt messages with your private key before sending.
  - Only your public key can decrypt the message.
  - If your public key opens the message, then it is from you.
  - Not for privacy.
- **Privacy:**
  - Get the recipient's public key and encrypt the message with it.
  - Only the recipient's private key can decrypt the message.
- Could use both methods and encrypt twice if you need both features

Basic H.235 Flow

- H.235 does not specify the actual authentication and encryption mechanisms, only the means to negotiate them.
- H.323 V.2 has the hooks to include it.
- Terminals must be configured a priori to secure the RAS and Call Signaling (H.225) channels (e.g., using IPSec).
- Authentication is provided by digital certificates
  - Authenticates the user, not just the terminal end-points.
- If a secure Call Control Channel (H.245) is required, it must be negotiated as part of the H.225 signaling.
- The secured H.245 channel is used to exchange symmetric encryption keys for the media.
- Media encryption: only the RTP payload is encrypted.

The Fast Connect Feature

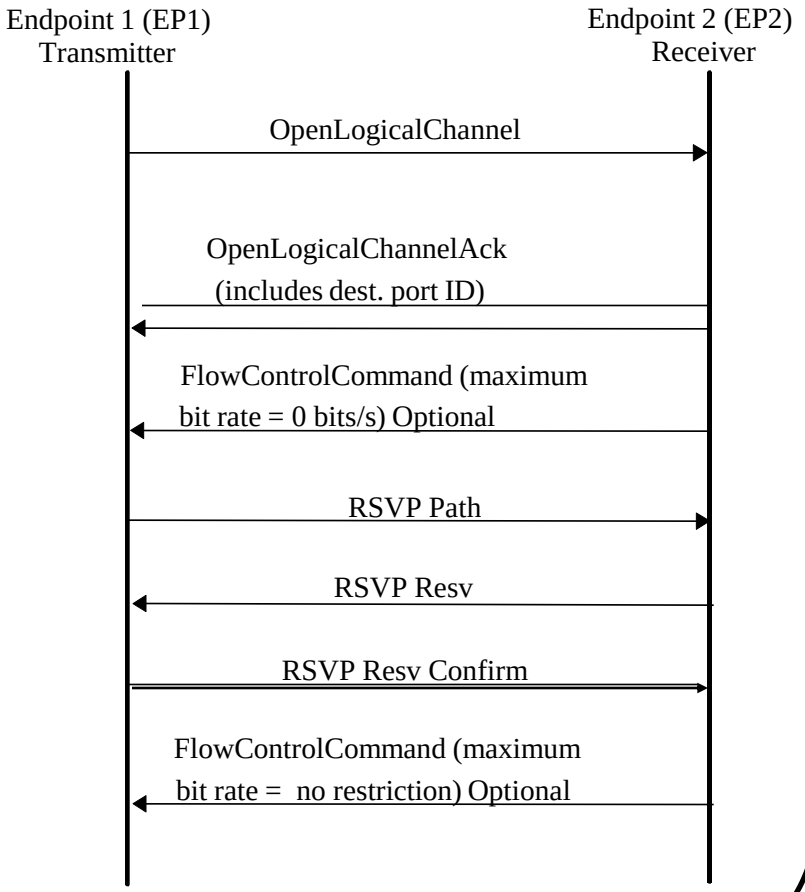
- Normal H.323 connect sequence:
  1. If a gatekeeper is present, negotiate admission (ARQ/ACF) using the H.225 RAS channel.
  2. If the call is allowed, open the H.225 Call Signaling channel and connect to the other side.
  3. If the other side accepts the call, open the H.245 Call Control Channel and negotiate call parameters.
  4. Start sending the media.
- Fast connect - essentially bypasses step 3.
  - In step 2, request Fast Connect.
  - If the destination accepts, it can start sending media right away, at the same time as it sends the acknowledgment.
  - Originator must be prepared to receive the media.

V.2 QoS Capabilities

- In the Admission Request phase of RAS, an endpoint may indicate its capabilities to reserve resources.
- In the Admission Confirm, the gatekeeper may indicate who is responsible for resource reservation:
  - endpoint-controlled
  - gatekeeper-controlled
  - no resource reservation (best effort)
- H.323 only communicates resource reservation information and capability between H.323 endpoints
  - Actual resource reservation must be done outside H.323 (e.g., with RSVP)
  - H.323 allows negotiation of resource reservation information and protocols in the H.245 Call Control step.

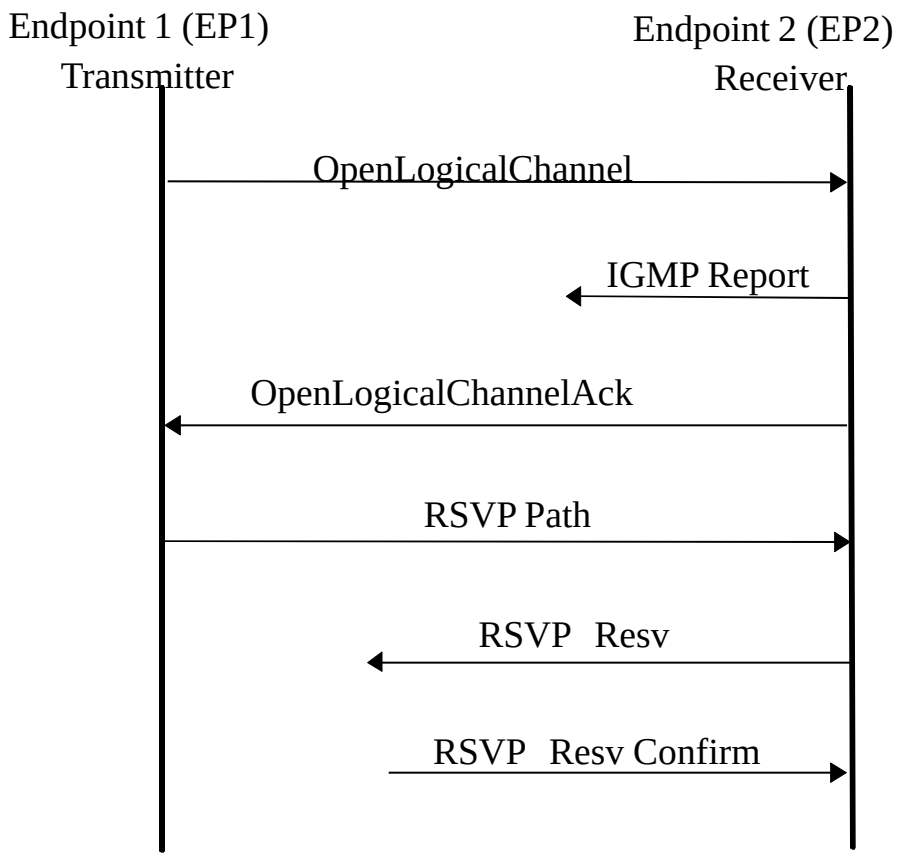
H.323 V.2 and RSVP

- The use of RSVP is negotiated during the H.245 Capabilities Exchange phase.
  - Note that in this phase what is decided is whether or not to use the protocol, not the actual stream parameters
- The actual RSVP exchange starts after the Logical Channel is opened.
- The RSVP reservation is removed right before the logical channel is closed.



RSVP and the Multicast Case

- The **OpenLogicalChannel** procedure is still point-to-point.
- After the Logical Channel is open, the receiver joins the multicast group and makes the reservation.
- Sender removes the reservation after the last receiver has left



RSVP Reservation Style

- H.323 requires the use of the ***Fixed-Filter*** style in all RSVP `Resv` messages because:
  - In the point-to-point case, the shared-filter reservations (Shared Explicit and Wildcard) reduce to Fixed Filter.
  - Different reservation styles for the same session cannot be merged by the network; e.g., in a multicast, if some receivers ask for FF and some for SE, either the FFs or the SEs will fail.
  - Shared reservations are suitable only for applications where not all the multicast sources transmit simultaneously; H.323 has no mechanisms to guarantee that.

Other H.323 V.2 Features

- **Pre-granted ARQ**
  - Allows a gatekeeper to pre-grant ARQs to an endpoint on registration to further reduce call setup time.
- **Overlapped Sending**
  - Allows the endpoint to send partial addressing information to the gatekeeper; call proceeds as enough addressing becomes available.
  - Used to reduce setup latency (by sending "digits" as the user dials them).
- **Alternate Gatekeeper**
  - The gatekeeper can give endpoints alternate gatekeeper addresses, in case this gatekeeper fails

Other V.2 Features (cont.)

- **Alternate Endpoint Address**
  - Endpoints can register alternate (backup) addresses with the gatekeeper.
- **Resource Availability**
  - A gateway can inform the gatekeeper of its call handling capability and current usage.
- **Media Enhancements**
  - Enhancements to H.263 signaling
  - Added support for GSM Audio Compression
- **Others**
  - Support for carrying DTMF
  - MCUs can provide conference lists to endpoints
  - Other protocol enhancements

New Features in H.323 V.3

Version 3 was approved in September of 1999 and adds a few small changes to Version 2. Features:

- **Re-using of TCP Connections:**
  - An endpoint can indicate that it is capable of using the same TCP connection for multiple calls.
  - This reduces the overhead of opening a connection per call, which may be significant for gateways.
- **Caller ID**
- **Language Preference**
  - The caller can specify the language it wishes to use; application is call centers and automated voice response systems.
- **Remote Device Control**
  - Ability to control remote devices (e.g., cameras) via H.282

New Features in V.3 (cont.)

- **Communication Between Administrative Domains**
  - Specified in H.225.0/Annex G.
  - Assumes that H.323 networks are organized in Administrative Domains for scalability purposes, and defines a protocol for communication between these domains.
  - Functions performed: address resolution; pricing exchange; call routing based on cost constraints; QoS.
- **Support for using UDP in call establishment**
  - Normally, H.323 uses TCP to establish the calls, which is acceptable for low volume of calls.
  - H.323/Annex E defines an alternative, UDP-based protocol for scalability

New Features in V.3 (cont.)

- **Simple Endpoint Type**
  - H.323 is a "heavy" standard, unsuitable for implementation in "small" hardware devices.
  - H.323/Annex F defines a "Simple Endpoint Type" (SET), which implements only a small subset of H.323 and is suitable for small hardware devices.
  - The SET is capable of establishing audio calls with other H.323 endpoints.
- **H.323 SNMP MIB (defined in H.341)**
- **Other services**
  - Call waiting
  - Message waiting
  - Call hold, park and pickup

New Features in H.323 V.4

H.323 Version 4 was approved in November 2000. The main added features address scalability, reliability and flexibility. New features:

- **Support for Multiplexed Streams**
  - Instead of running separate audio and video streams, run a single stream with audio/video multiplexed.
  - Simplifies audio/video synchronization.
- **Alternate Gatekeepers**
  - Builds on the Alternate Gatekeepers feature introduced in V.2, and adds a feature whereby an endpoint can declare its support for this feature.
- **Additive registrations**
  - Allows endpoints to use multiple RRQs to register aliases.

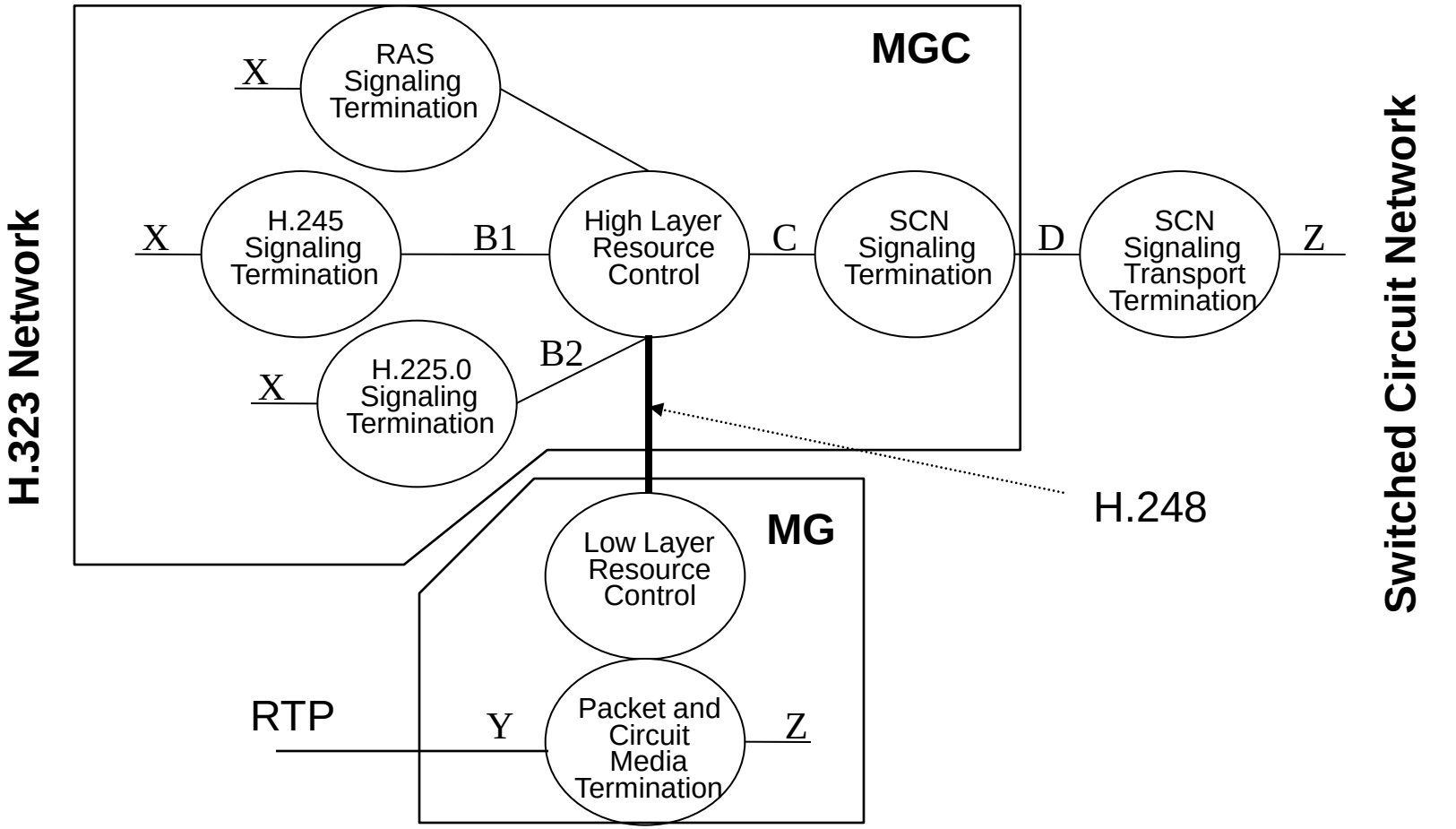
V.4 Gateway Decomposition

- Basic idea: "decompose" the gateway into different functional blocks.
- Very large gateways can be implemented by spreading these functional blocks over multiple physical devices.
- Interfaces are standardized so that multi-vendor gateways can be built; new H.248 Recommendation introduced for this purpose.
- The Gateway is decomposed into:
  - Media Gateway Controller (MGC)
  - Media Gateway (MG)

Gateway Decomposition

- Media Gateway Controller functions:
  - handle H.225.0 RAS messaging with an external gatekeeper
  - optionally handle the SS7 signaling interface
  - optionally handle the H.323 signaling interface
  - High-level resource management
- Media Gateway functions:
  - terminates the IP network interface
  - terminates the Switched Circuit Network span
  - Low-level resource and hardware management
  - may handle H.323 signaling in some physical decompositions
  - may handle the Switched Circuit Network signaling in some physical decompositions.

Gateway Decomposition Diagram



V.4 Supplementary Services

- **H.323/Annex K:**
  - Provides HTTP-based control of H.323 services.
  - Third party call control mechanism that utilizes a separate HTTP connection for control
- **H.323/Annex L:**
  - Using this, an H.323 device may communicate with a "feature server" to provide the user with various services
- **Other Supplementary Services:**
  - Call completion, call offer, call intrusion, enhanced caller ID.

Other V.4 Features

- **Usage Information Reporting**
  - Gatekeeper may request usage information during the call for accurate billing.
  - Important when calls are not routed through the gatekeeper.
- **Endpoint Capacity Reporting**
  - Endpoints can precisely report their capacity and usage.
  - This information can be used by the gatekeeper to properly route calls and avoid congested gateways, for example
- **Bandwidth Management**
  - Endpoints are required to signal their bandwidth requirements accurately and reduce it if they are not using the negotiated amount.
  - Additional IIR messages to allow the gatekeeper to properly manage bandwidth in a multicast call.

Other V.4 Features (cont.)

- **Enhanced FAX support**
  - Calls can start as voice and then switch to FAX.
  - FAX data can be carried both over TCP and UDP.
- **Tunneling of SCN Signaling**
  - Employed when the H.323 network is used to connect two SCNs.
  - The SCN signaling can be carried opaquely
- **H.245 in Parallel with Fast Connect**
  - The H.245 negotiation can be started at the same time as the Fast Connect procedure.
  - Endpoints will connect more quickly if Fast Connect fails.
- **H.323 URL**
  - Defined as `h323:user@host`; "user" is the user or service, and "host" is the location (gatekeeper, endpoint, etc.)

Other V.4 Features (cont.)

- **Call-Credit Related Capabilities**
  - Used to support “pre-paid access”.
  - Extensions to the RAS messages to indicate to the gateway the necessary information.
- **Support for DTMF Relay over RTP**
  - Uses RFC 2833 to convey precise DTMF information (digits and timing)
  - Useful when this information is relayed through the gatekeeper but the gatekeeper is not interested in the information.