H.323 continued

Anjali Agarwal

H.450 Supplementary Services

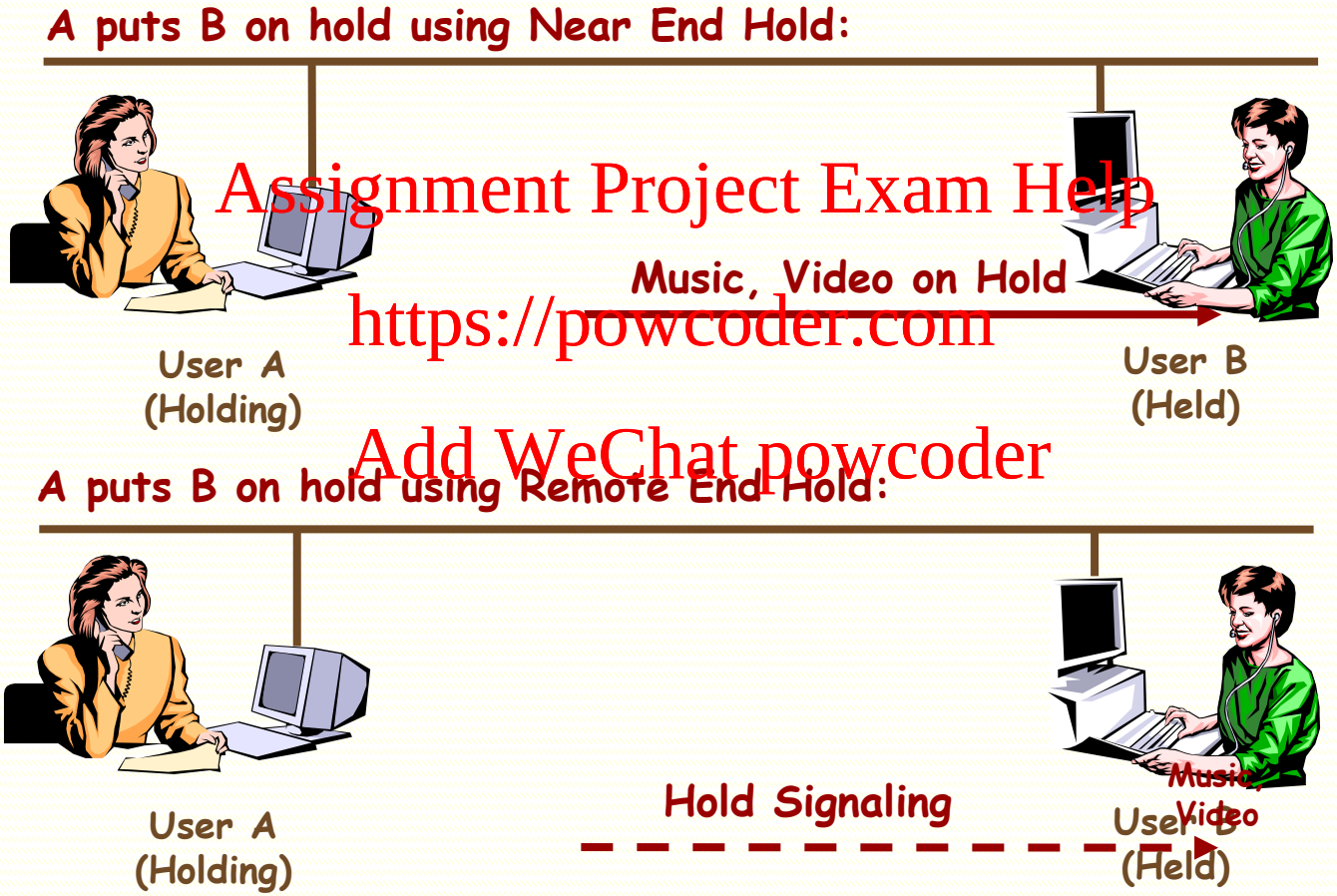
Functions in addition to a “basic call”, e.g.:

- Transfer calls, Consultation Transfer, Alternating (H450.2)
- Forward calls (diversion) (H450.3)
- Hold a call and take or make another (consulting) (H450.4)
- Work group functions: Park and Pickup a call (H450.5)
- Indicate that another call is waiting (H450.6)
- Message waiting indication (H450.7)
- Name identification (H450.8)
- Call completion on busy or on no reply (H450.9)

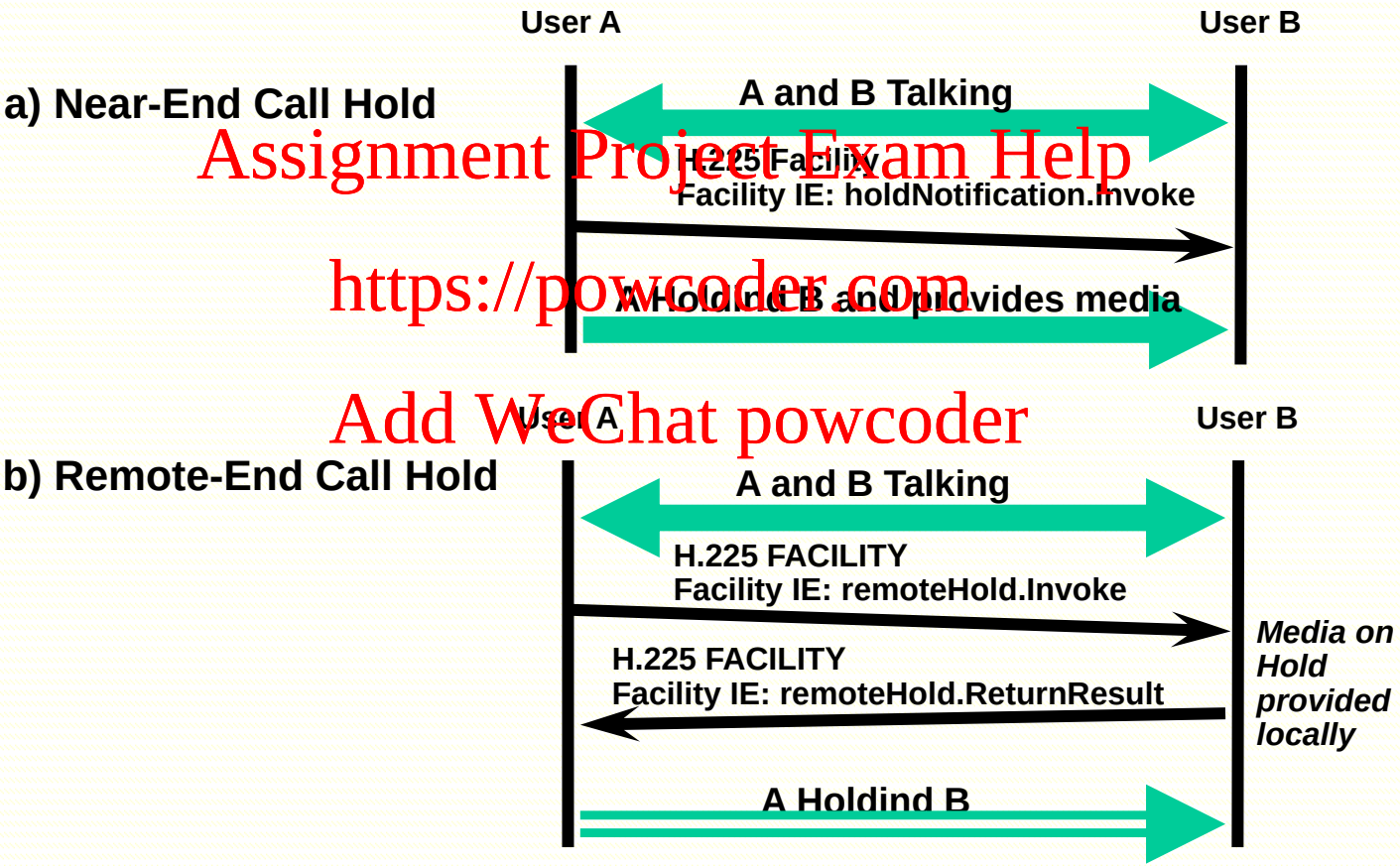
THEY ALL NEED SIGNALING OVER THE NETWORK

FUNCTIONAL COMPONENTS

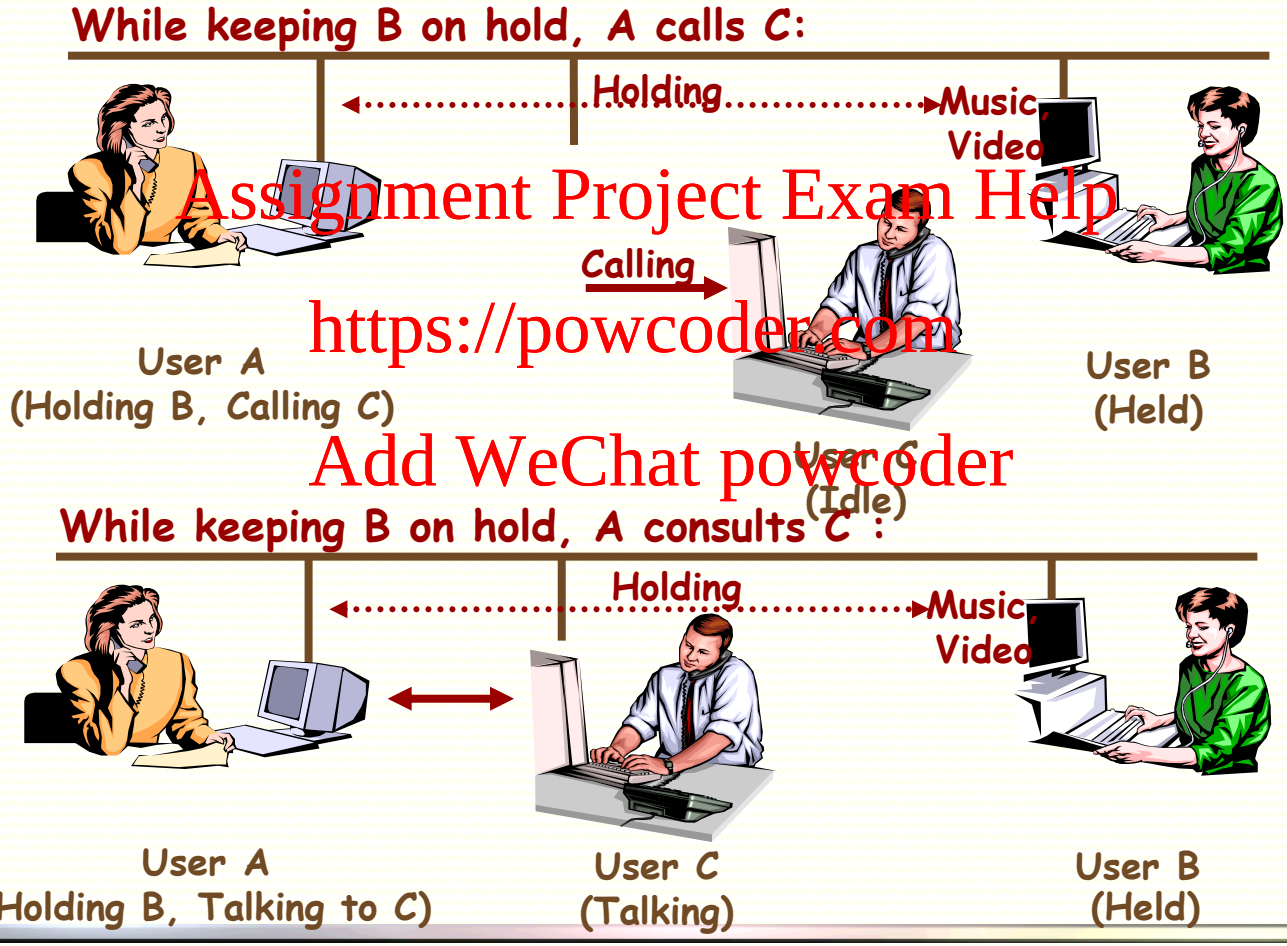
Usage Scenario: H.450.4 Call Hold



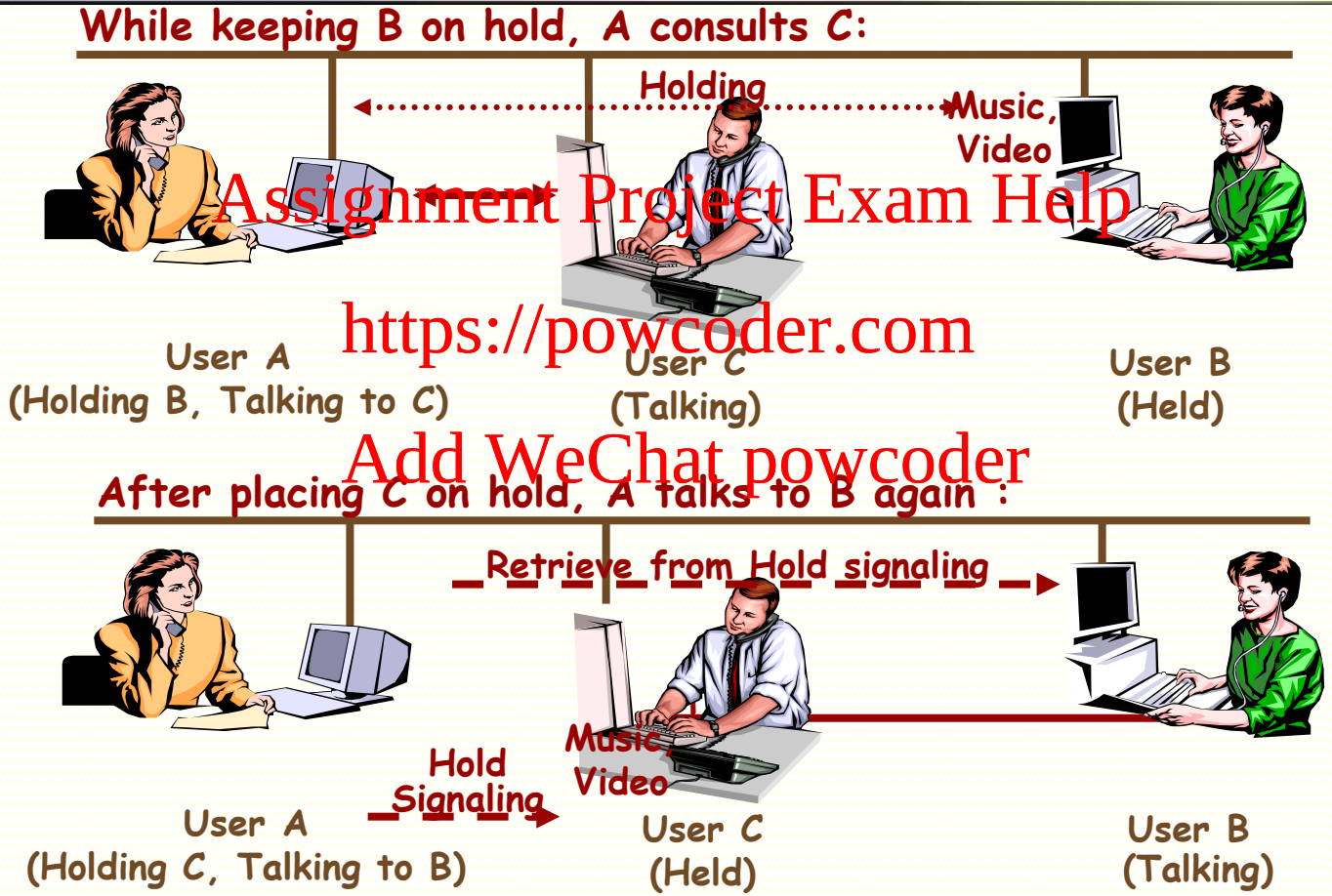
H.450.4 Call Hold Signalling



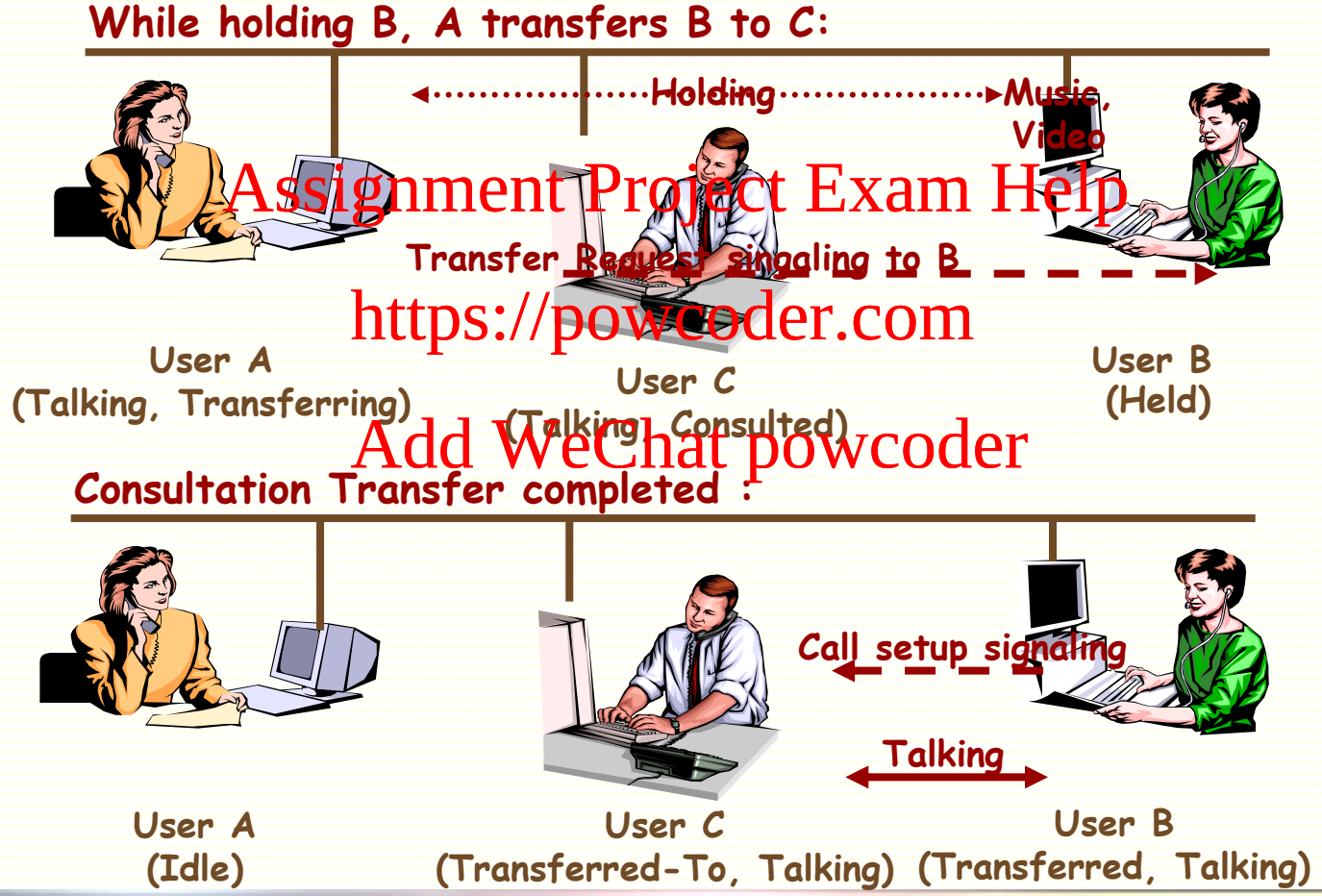
Usage Scenario: H.450.2 Consultation



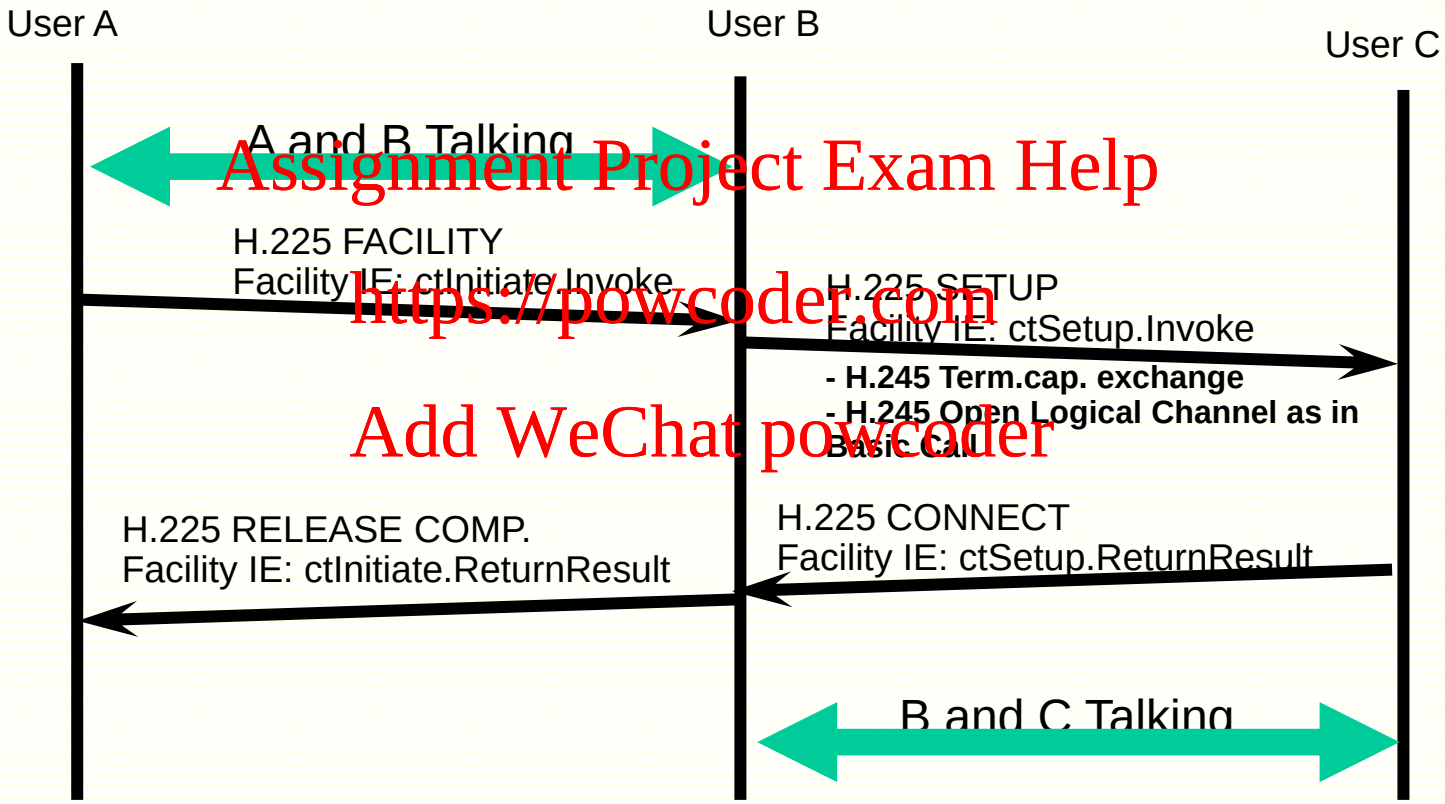
Usage Scenario: H.450.2 Alternating



Usage Scenario: H.450.2 Consultation Transfer

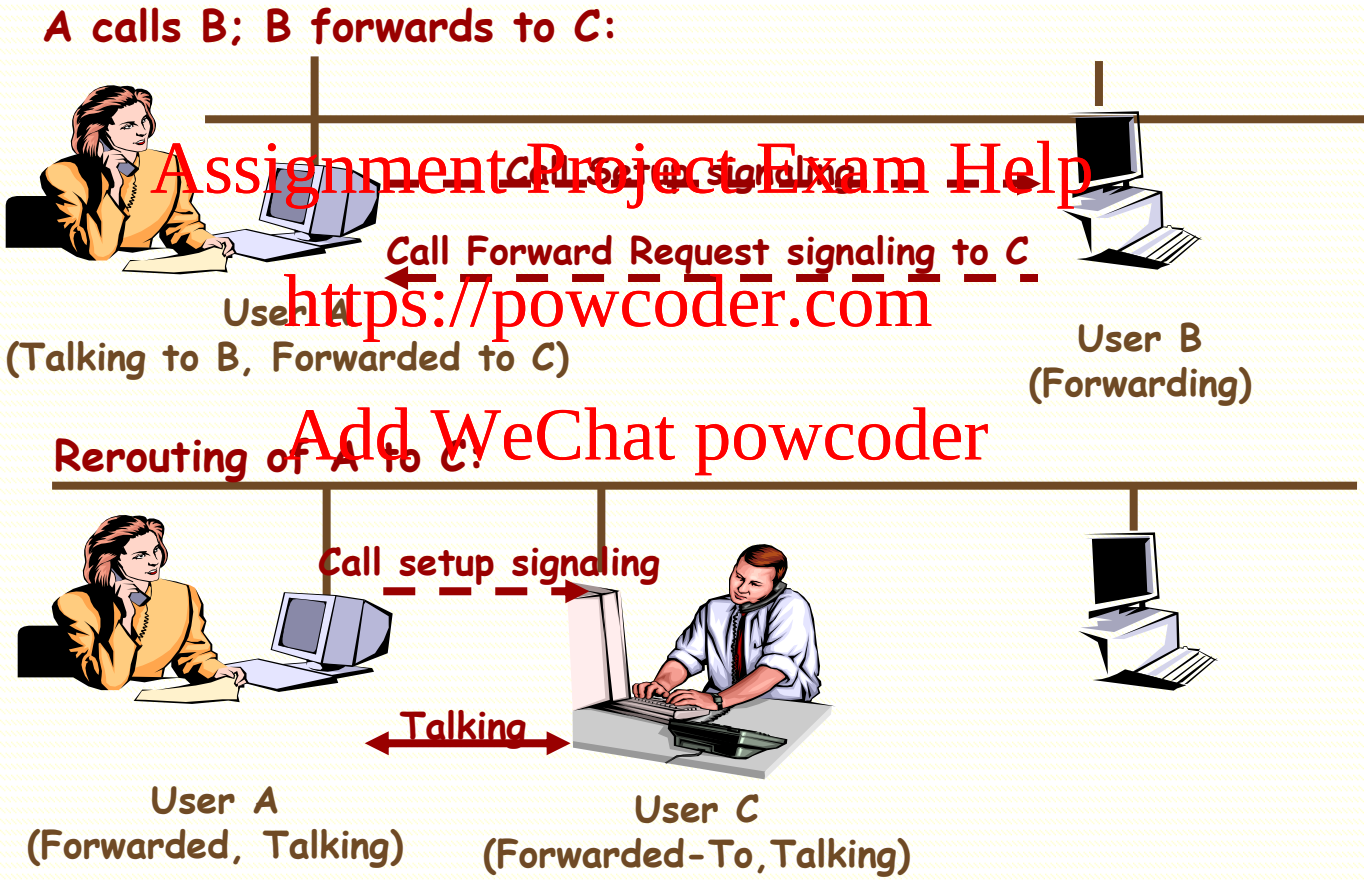


Usage Scenario: H.450.2 Call Transfer Signalling

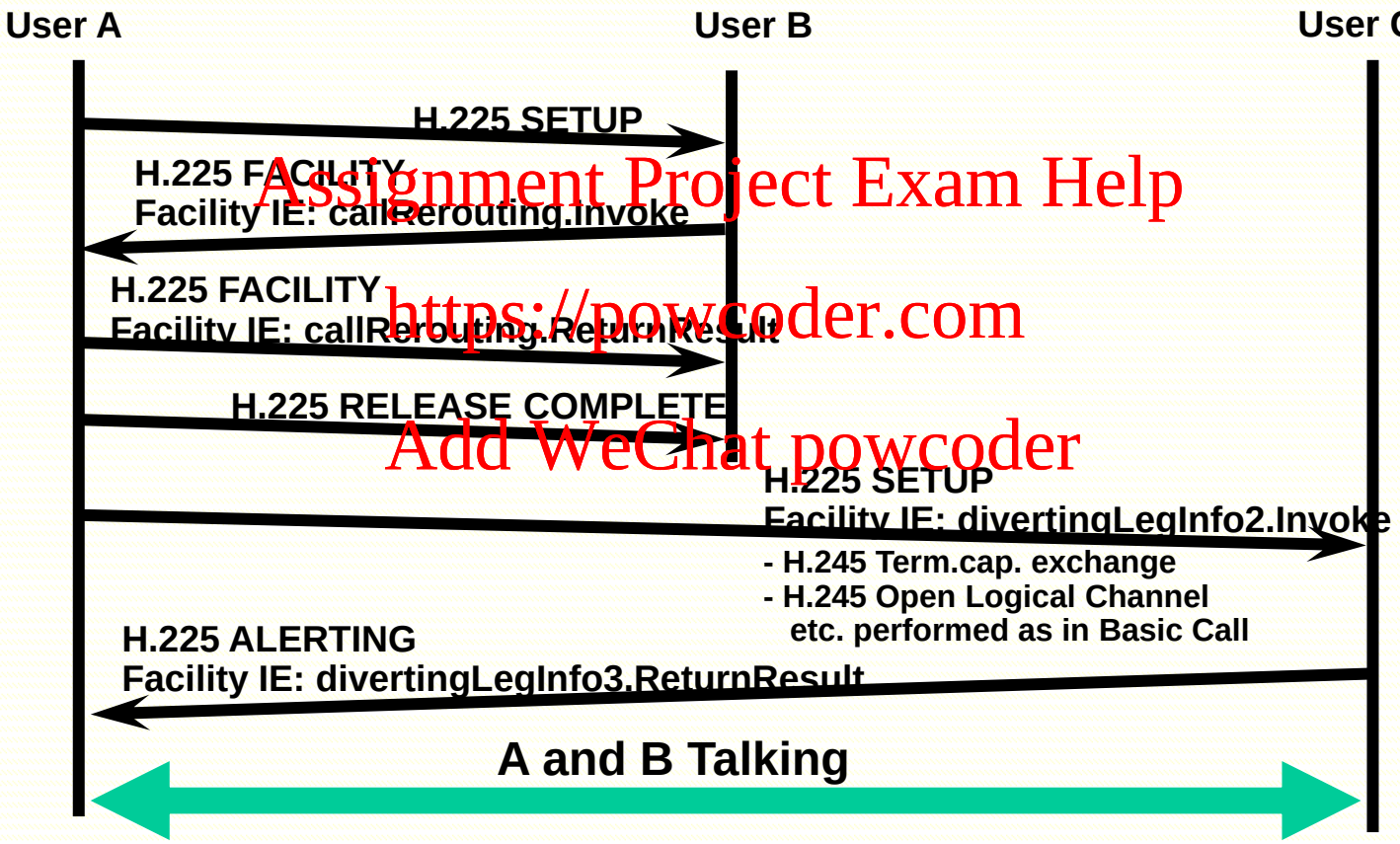


A transfers B to C

Usage Scenario: H.450. 3 Call Forwarding



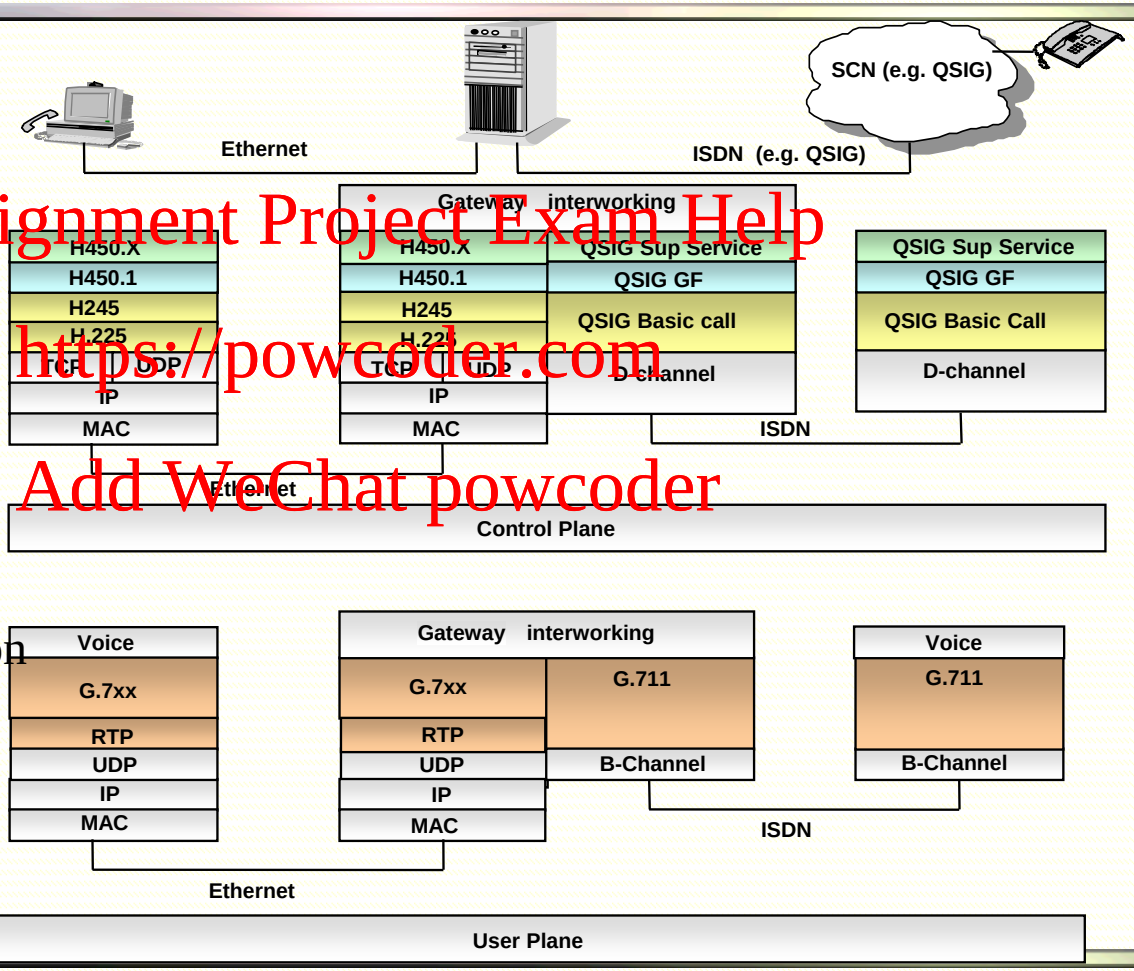
Usage Scenario: H.450.3 Call Forward Signaling



A calling B, who is forwarded to C

H.323/H.450 Gateway Interworking Layers

- H.450 based on QSIG concepts
- Corresponding functions in both worlds allow mapping, interworking
- Smooth migration of LAN - PBX world



"Local Features" using plain H.323

Local Endpoint functions:

- Repeat a call
- Personal directory
- Speed dialing
- Multiple virtual lines
- Privacy Functions (Do Not Disturb, mute, …)
- Send Email to the caller

Gatekeeper Based

- Block Calls (Long distance, International, Outgoing, Incoming, etc)
- Call Detail Recording
- Treatment of terminals out of service
- etc.

THESE ARE POSSIBLE WITH "PLAIN" H.323 AND DO ***NOT*** NEED SUPPLEMENTARY SERVICES

Real time teleconferencing over the Internet

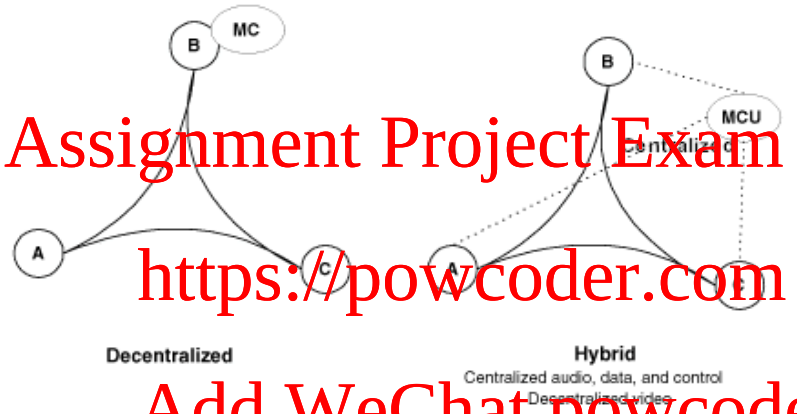
Point-to-point teleconference:

- » *gatekeeper really isn't necessary, since the two terminal endpoints can communicate directly*
- » *Gatekeepers may be used to allocate bandwidth for point-to-point conference services; or to use name aliases or "phone numbers" in a zone directory*

Multipoint teleconference:

- » *Gatekeeper and a MC/MCU is used for conferencing between multiple sites*
  - – **Centralized multipoint conferences**
    - – requires commonly accessible MCU
    - – audio, video, data, and control streams send in a point-to-point fashion to the MCU
  - – **Decentralized multipoint conferences**
    - – makes use of multicast technology

Real time teleconferencing over the Internet (cont.)



Decentralised (cont.):

- *MC is built into Client B's terminal endpoint that executes the call*
- *All terminals multicast audio and video to other participating terminals without sending the data to an MCU*
- *MP function on each node would mix and present the incoming audio and video signals to the user*
- *network must be configured to support multicast*

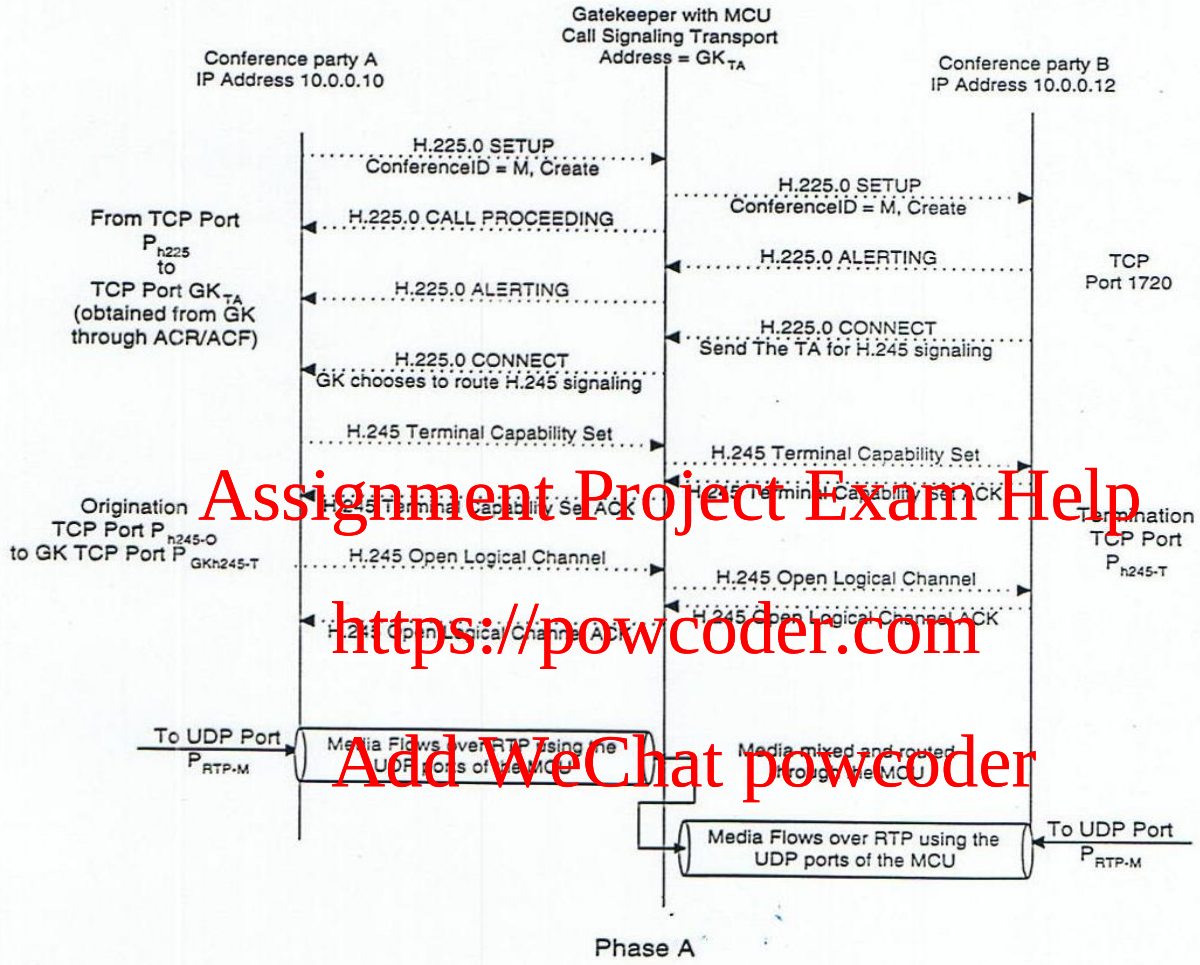
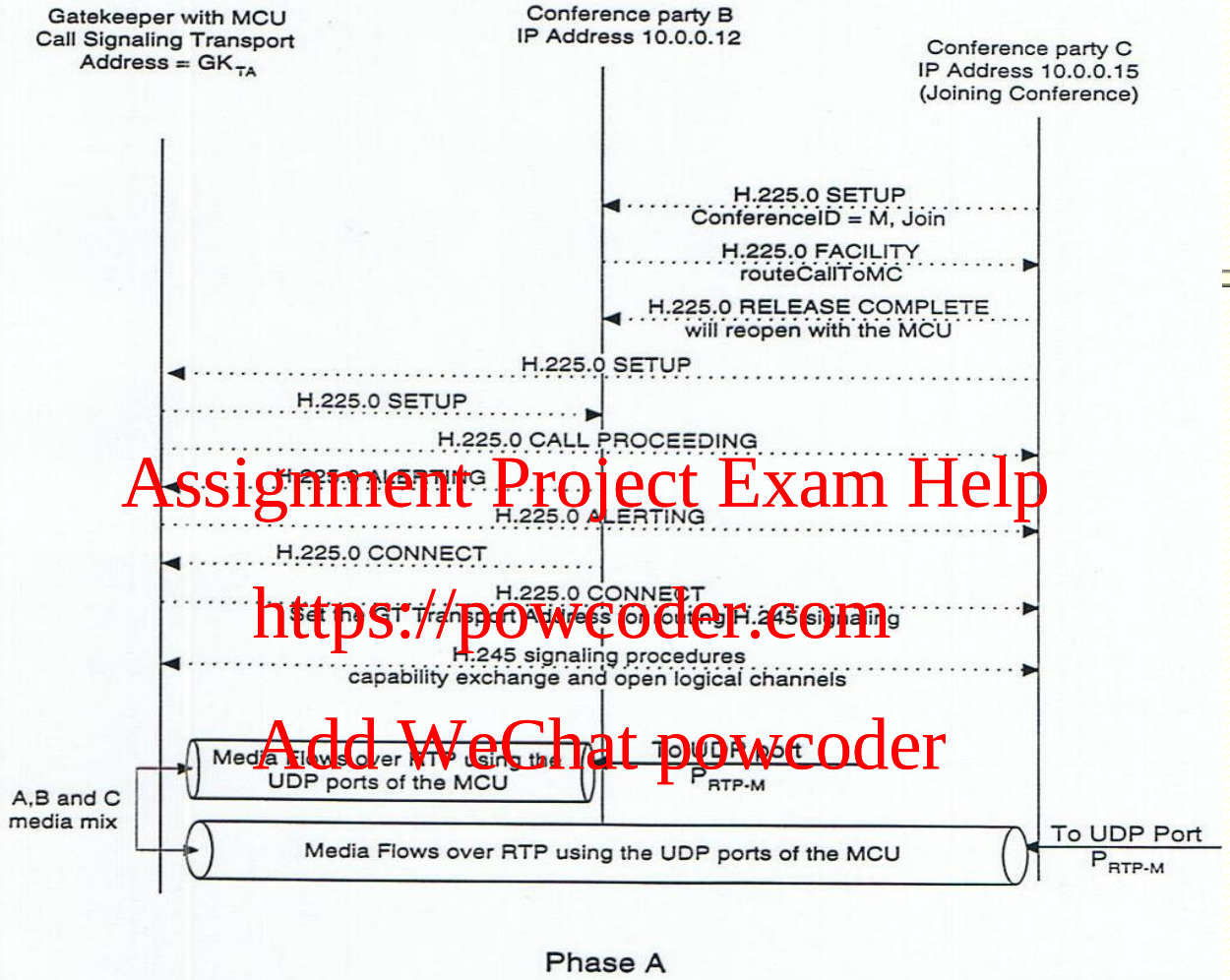


FIGURE 1.21 H.323 Gatekeeper Routed Conference Call Model, Initiation

15a



Phase A

FIGURE 1.22 H.323 Conference Call Model, Third Party Joins the Call

15 b

Firewalls and H.323

Conferencing with colleagues on the same LAN is relatively simple, because few security devices are installed inside the LAN, and internal routers know all endpoint IP addresses.

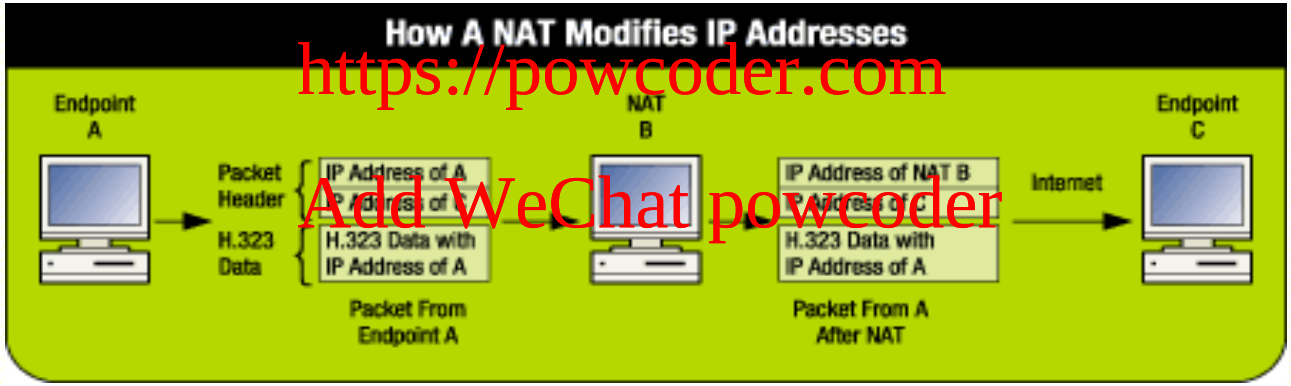
Conferencing over the public Internet with people who are on different LANs or ISPs is much more difficult, due to firewalls and network address translation devices.

Firewalls

- *examine the IP address and destination port of each data packet received from the outside world. If the firewall determines that the destination computer did not first initiate a request for data on that port number, it will typically discard the incoming data packet unless the port has been "opened" to receive unsolicited data*
- *H.323 requires that the firewall must allow unsolicited packets to enter the network and be routed to the receiving endpoint. Once the call parameters are negotiated, additional ports must be opened to receive the audio and video information from the originating endpoint, further compromising the firewall. Consequently, many network administrators perceive external H.323 calls as network security threats*
- *H.323-compliant firewalls understand H.323 protocols, and safely open ports to receive H.323 Internet calls*

NATs and H.323

Companies and ISPs use network address translation (NAT) to conserve routable IP addresses. A NAT converts the private IP address used within an internal network to a different public IP address when connecting to services on an external network, such as the Internet, allowing the organization to use a small number of public IP address in its communication with the world.



the IP address of the H.323 endpoint behind the NAT initiating the call is embedded within the H.323 data stream, and the receiving endpoint tries to send its audio and video data back to the initiating endpoint's IP address. Because this address is unknown to the routers, packets are simply discarded somewhere in the Internet.

H.323 endpoints outside the NAT cannot call someone whose LAN or ISP uses NAT

The Fast Connect Procedure

- For call establishment appeared in version 2
- Offers significant improvement over standard call setup
- Point-to-point call setup with as few as two messages
- Open Logical Channel (OLC) structures are included in the SETUP command
- OLC Ack structures response with:
  - *Call proceeding*
  - *Alerting*
  - *Progress*
  - *Connect*
- Fast connect procedures must be agreed to by both endpoints, otherwise full H.245 is used
- Call Termination using *faststart* is done with a single RELEASE COMPLETE message

H.235 (Security)

Common security requirements:

Authentication –

- *user involved in a conference call is indeed whom they claim to be*
- *gateways, gatekeepers and MCUs should also be authenticated*

Privacy and Confidentiality –

- *network can be tapped*
- *media stream data, and also the signaling data should be confidential*
- *use encryption and decryption techniques to hide data*

H.235 (Security)

Integrity –

- *All the signaling messages and media streams passing between different elements should be uncorrupted, since crackers may try to make unauthorized modifications to the information sent between two entities A and B*
  - encryption key that A sent to B may be modified by the hacker.
  - Now B will start the encryption using the wrong key and the data can thus be decrypted by the hacker and they can encrypt the data again using the correct key.

Nonrepudiation –

- *The user should not be able to deny that he has been involved in a conference call*
- *user needs to be assured that service provider will not charge him for conference calls that he has not been involved in*

Availability –

- *services provided will have to be ensured of certain level of availability, to minimize the DOS (Denial Of Service) threat*