Connection-Oriented Media Transport in SDP

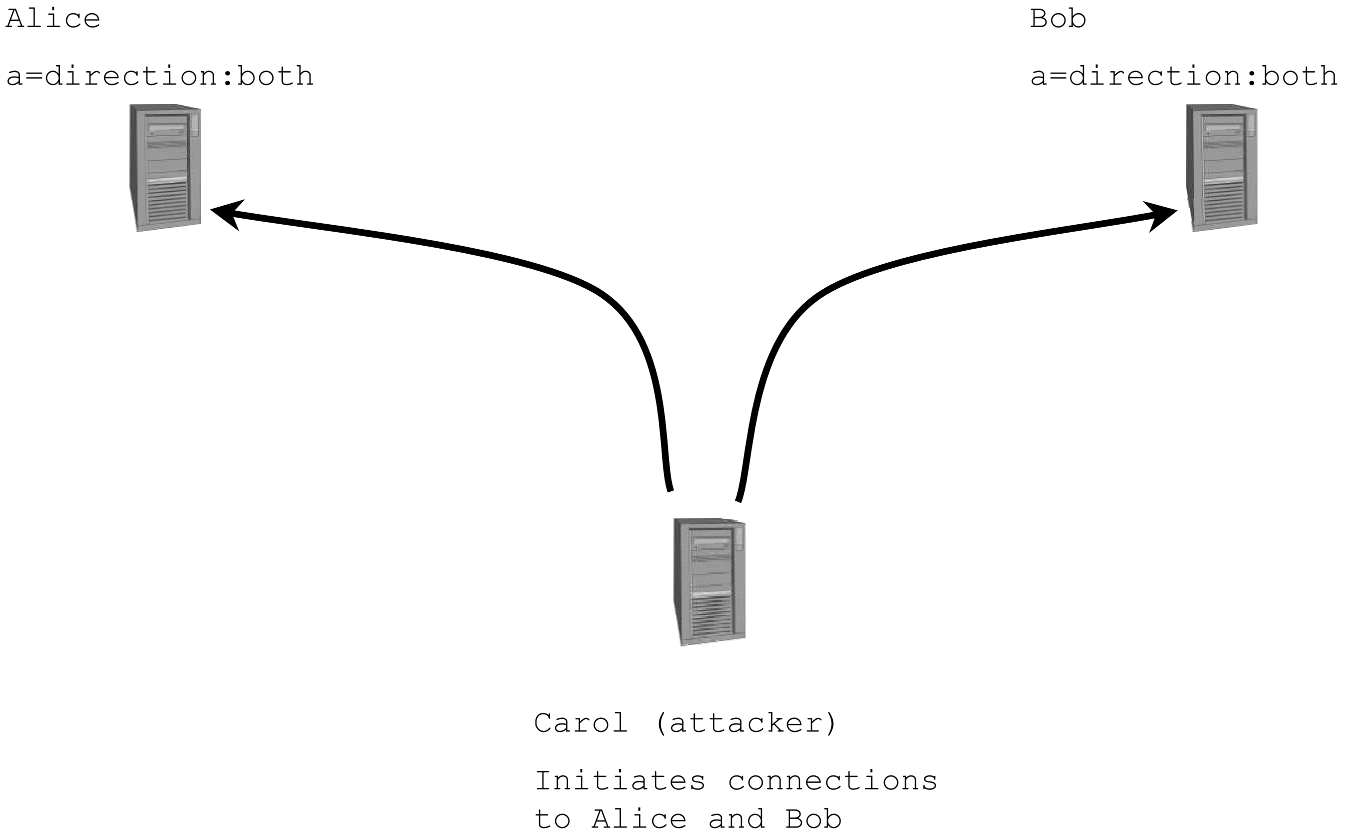
draft-ietf-mmusic-sdp-comedia-05.txt

David Yon

Changes made to comedia-05

- Removed source address/port per resolution of the MMUSIC chairs
- Removed current security considerations section in prep for -06

The issue raised by comedia-fix



Alice

a=direction:both

Bob

a=direction:both

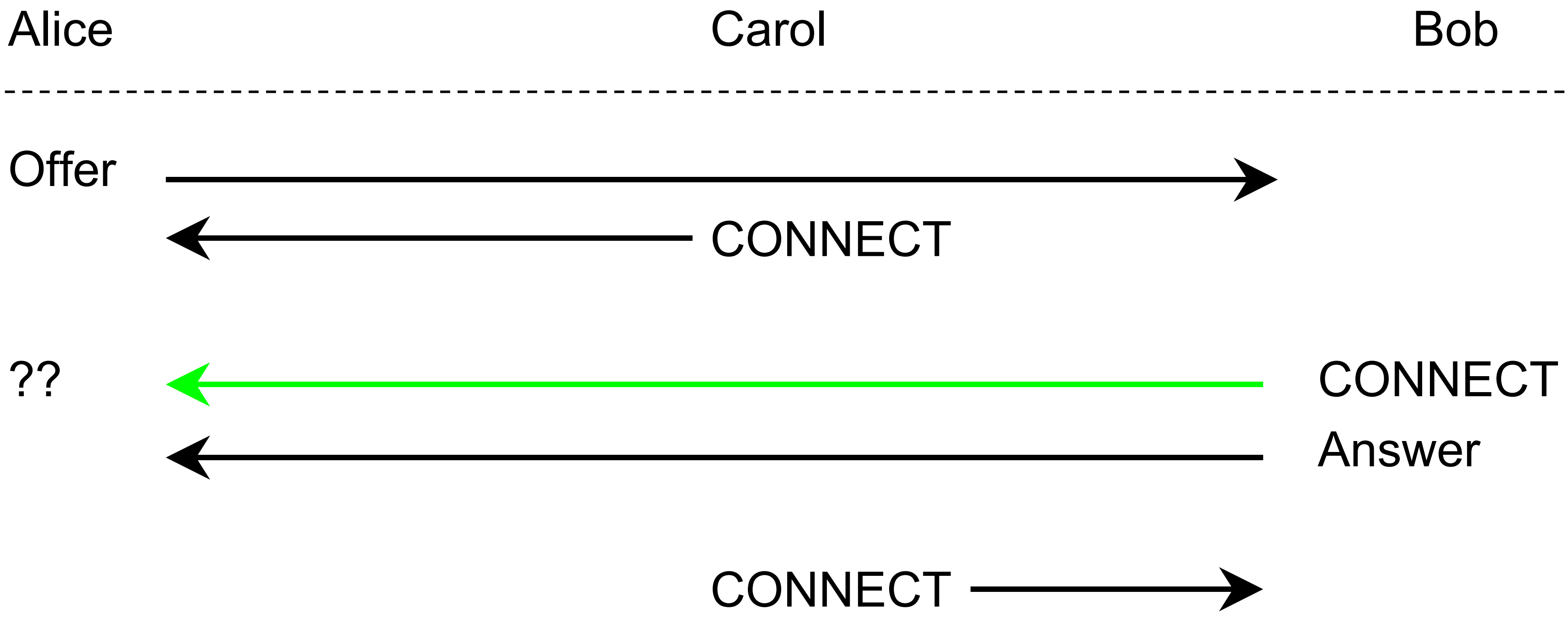
Carol (attacker)

Initiates connections
to Alice and Bob

Defenses Against Hijacking

- The most robust defense is secure media streams
- Attack can be downgraded to Denial of Service
  - Endpoints MUST follow rules in Section 4 (b) and (c)
  - Duplicate incoming connections act as a tripwire
  - Extend listener lifetime to detect duplicate connections
  - Works for both TCP and bidirectional RTP/AVP

Scenario 1: Full Connectivity



Alice

Carol

Bob

Offer

CONNECT

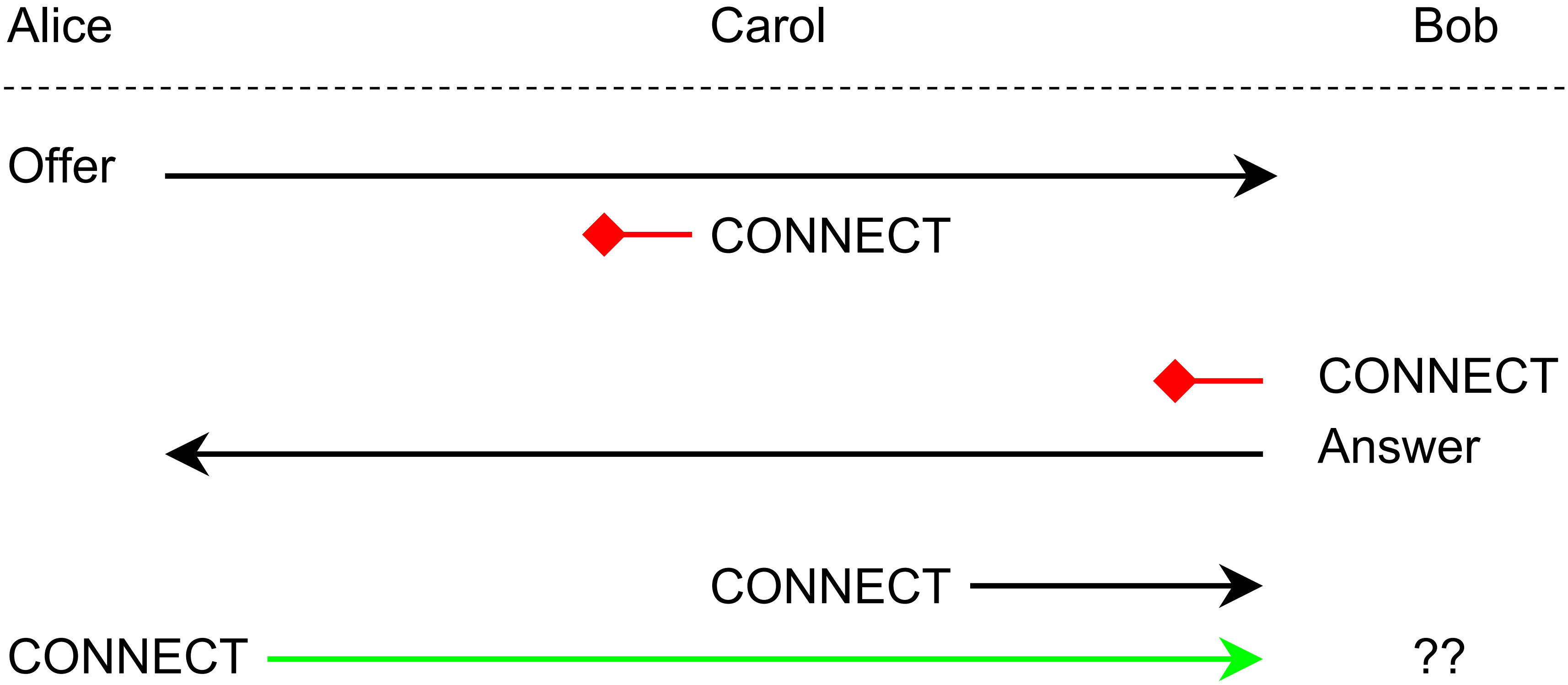
??

CONNECT

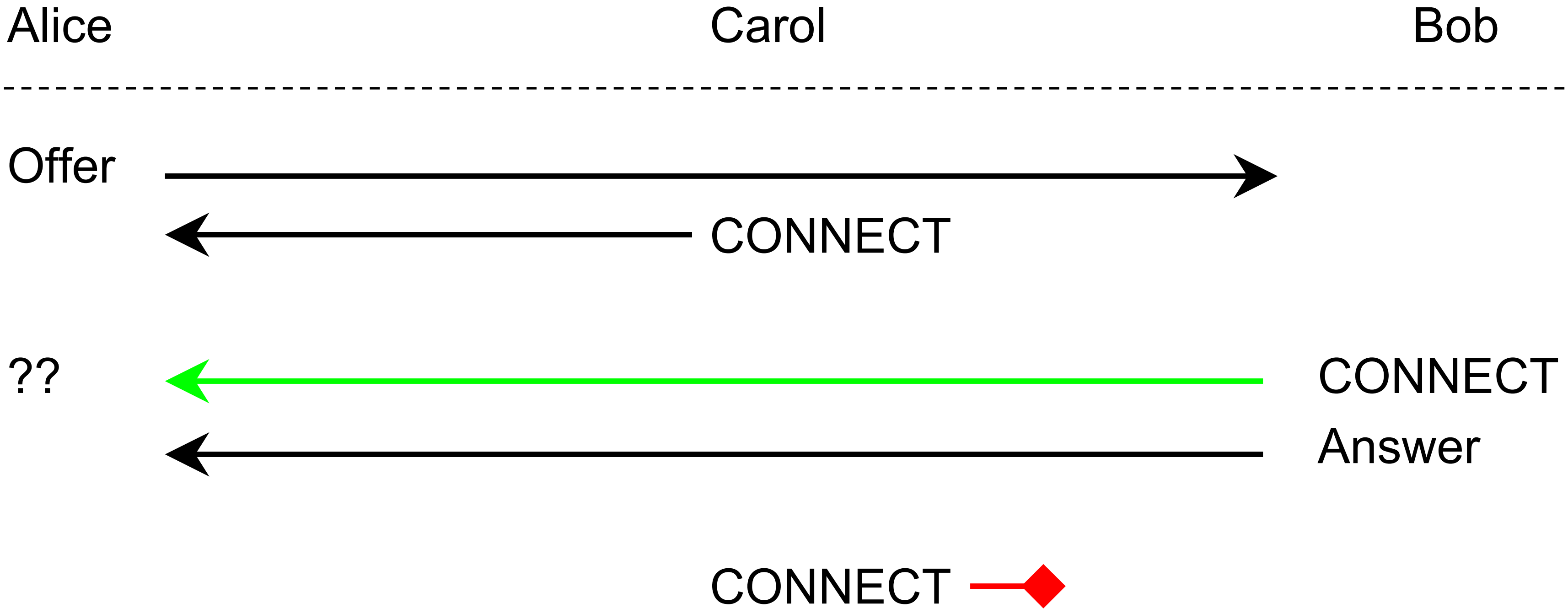
Answer

CONNECT

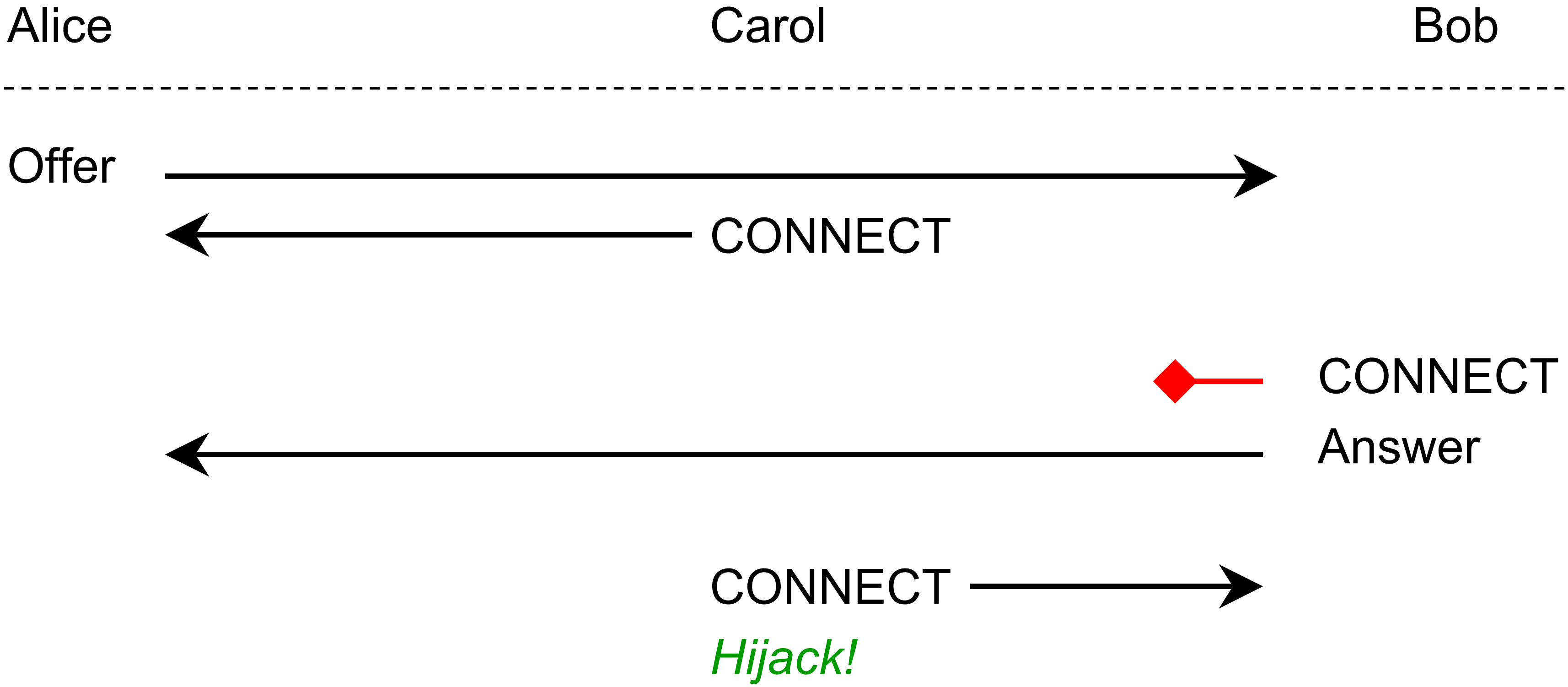
Scenario 2: Bob/Carol can’t connect to Alice



Scenario 3: Alice/Carol can’t connect to Bob



Scenario 4: Bob can’t connect to Alice



Alice

Carol

Bob

Offer

CONNECT

CONNECT

Answer

CONNECT

Hijack!

Mitigating Scenario 4

- Correlates to a common client/server topology:
  - Client (Alice) is behind NAT/Firewall
  - Server (Bob) is on public Internet
- Bob may therefore know he’s fully routable
  - So don’t offer “both”, offer “passive”
  - This prevents Alice from accepting Carol’s connection

Next Steps

- Recent RTSP issues on the list, need to come to closure
- Publish comedia-06 with expanded security section
- IETF Last Call? (please?)