UNC INFORMATION TECHNOLOGY SERVICES

The new ITU Standards for H.323 Firewall and NAT Traversal

Christian Schlatter, cs@unc.edu

FW/NAT vs P2P

- FW policies and NAT boxes are designed for Client-Server applications
  → only outgoing connections

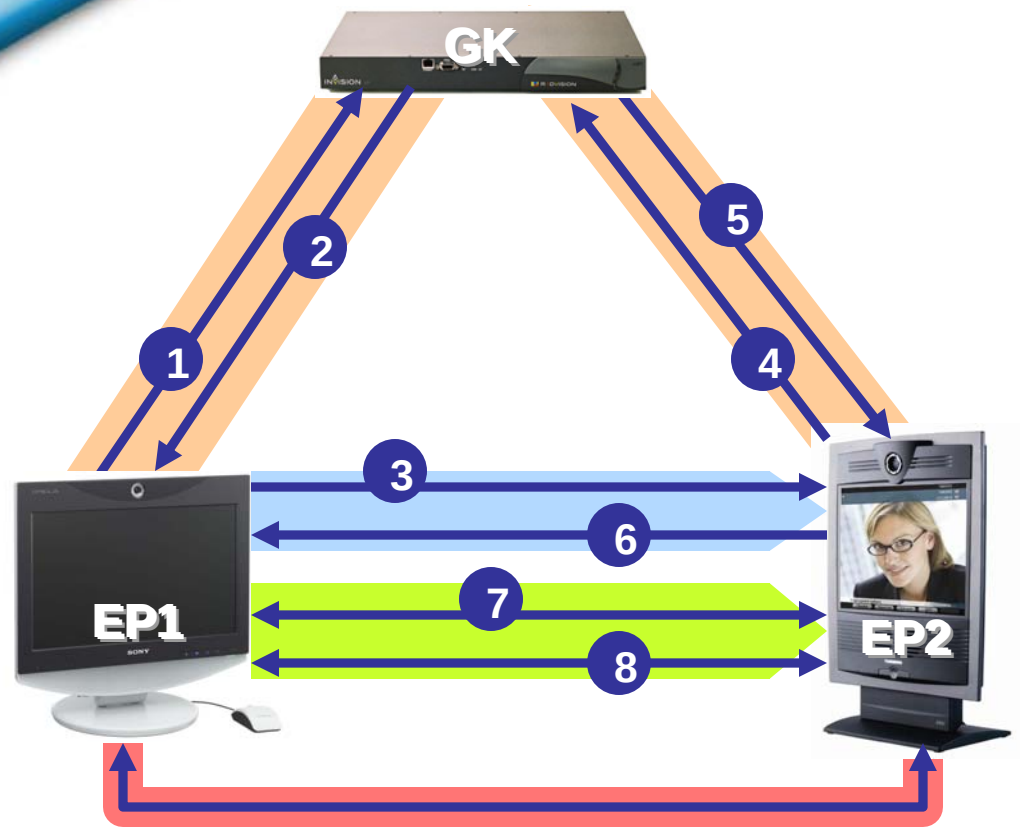
- FWs and NATs destroy Internet end-to-end transparency
  - we have to live with that ☹

H.460.17/18/19

- Vendors developed proprietary FW/NAT traversal solutions (Ridgeway, Expressway, PathFinder, V2IU, …)
- ITU-T ratified H.460.17/18/19 in summer 2005

	H.460.17	**H.460.18**	**H.460.19**
Traffic type	**Signaling** (H.225/H.245)	**Signaling** (H.225/H.245)	**Media** (RTP)
Main Contributions	Radvision	Tandberg Radvision Polycom	Radvision Tandberg Polycom

Reminder: H.323 Call Establishment



1 ARQ (dest alias, bw)
2 ACF (dest H.225 addr)
3 Setup
4 ARQ (bw)
5 ACF (bw)
6 Connect (dest H.245 addr)
7 Caps exchange, master/slave
8 Open logical channels (RTP transport addresses)

RAS (H.225): UDP, port 1719
Call Signaling (H.225/Q.931): TCP, port 1720
Call Control (H.245): TCP, negotiated port
Media Streams (RTP): UDP, negotiated ports

H.323 Channels

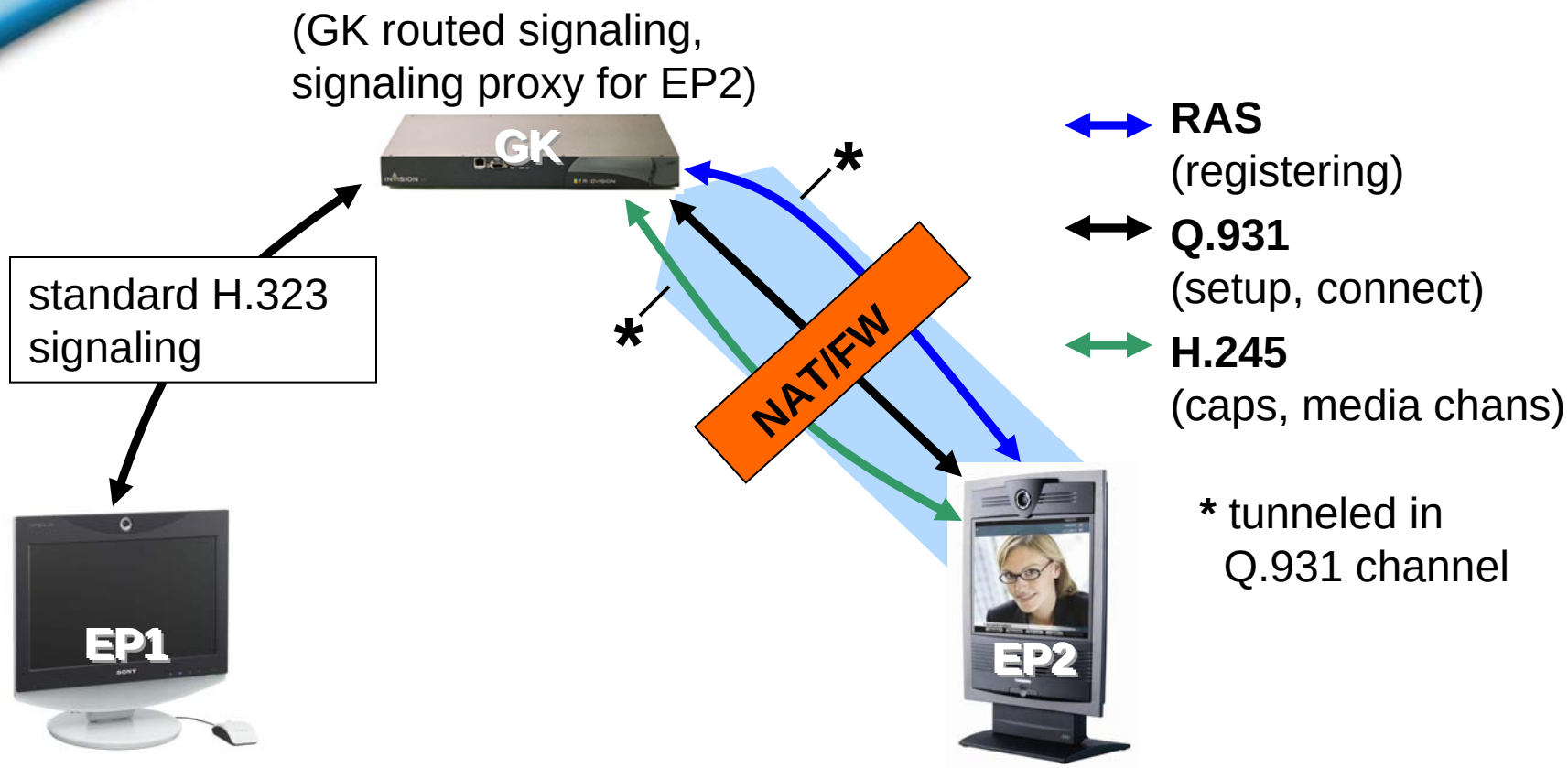
- ➔ Three signaling channels (RAS, Q.931, H.245)
- ➔ Multiple media channels

All of these channels must traverse NAT/FW

FW/NAT Traversal Techniques

- TCP
  - (persistent) outgoing connection to rendez-vous server
  - Connection re-use for incoming calls
  - Keep-alive messages
- UDP
  - Pinholes (create FW/NAT mapping with outgoing message, use the mapping for incoming traffic)
  - Symmetric UDP traffic (e.g. RTP)
  - Keep-alive messages

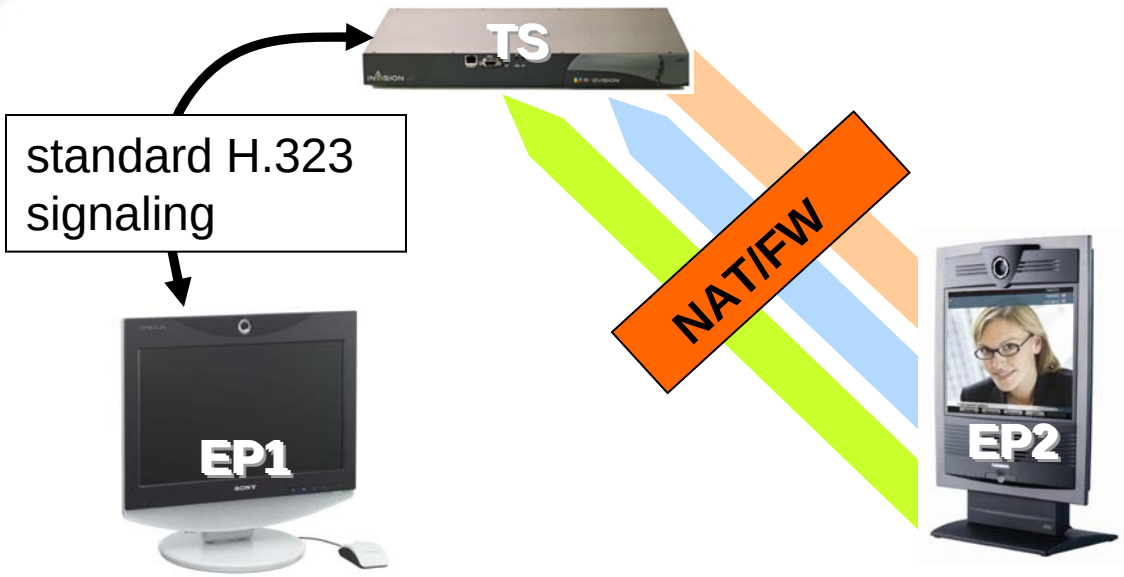
H.460.17 ("RAS over H.225")



Persistent H.225/Q.931 connection: TCP, port 1720
- opened upon first registration by endpoint
- keep-alive messages (RRQ/empty TPKT)

H.460.18

(**T**raversal **S**erver =
GK + H.225/H.245 signaling proxy)



Q.931 for Incoming Calls

1) TS sends **RAS SCI** (Incoming Call Indication) to EP2
2) RAS SCI triggers outgoing TCP for Q.931

H.245 for Incoming Calls

1) TS sends **H.225 startH245** to EP2
2) startH245 triggers outgoing TCP for H.245

RAS channel, RRQ opens pinhole, **symmetric UDP**, RRQ keep-alives

Q.931 channel, **outgoing TCP**:1720, empty TPKT keep-alives

H.245 channel, **outgoing TCP**:<negotiated>, empty TPKT keep-alives

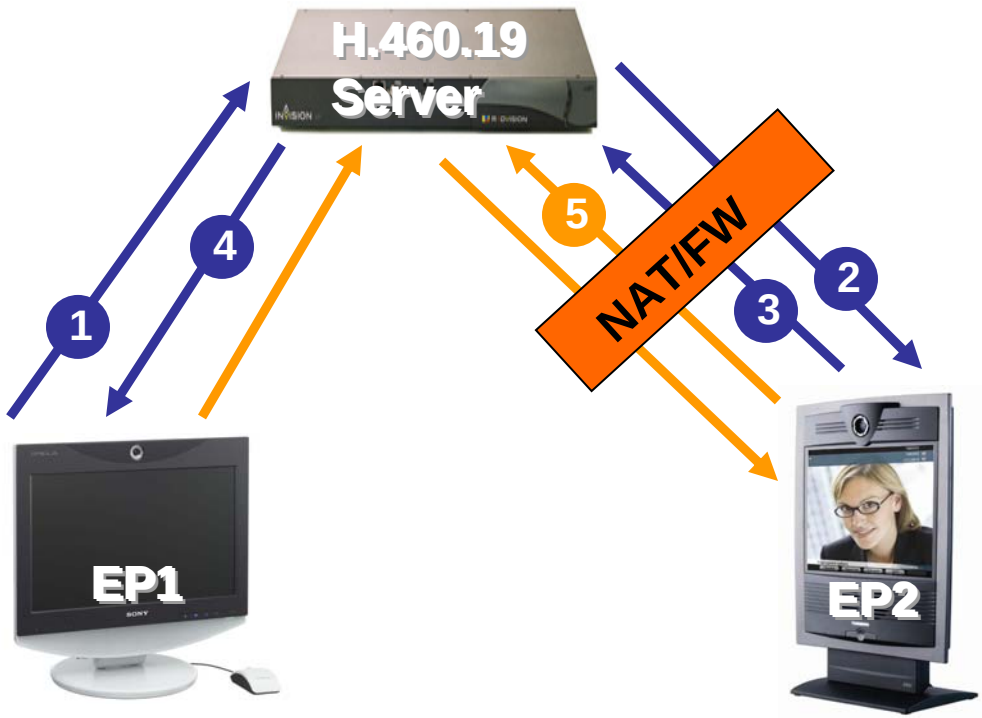
H.460.19

- H.460.19 Server alters H.245 RTP transport addresses to stay in the media path (RTP relay)
  → H.460.19 needs an established e2e H.245 channel (H.460.18)

- Outgoing keep-alive messages (RTP packets with empty payload) open pinhole for incoming RTP

- Outgoing RTCP packets open pinhole for incoming RTCP packets (RTCP is bi-directional)

H.460.19: Incoming RTP



1 OLC Request

2 OLC Request
(KeepAlive RTP addr = IP_S)

3 OLC Response
(RTP addr = IP_2)

4 OLC Response
(RTP addr = IP_S)

5 KeepAlive RTP
(opens pinhole,
sent every 5-30s)

H.245 traffic

RTP traffic

OLC = H.245 OpenLogicalChannel
(RTCP not shown)

H.460.19: Multiplexing RTP

- Multiple RTP/RTCP sessions can use a single pair of transport addresses

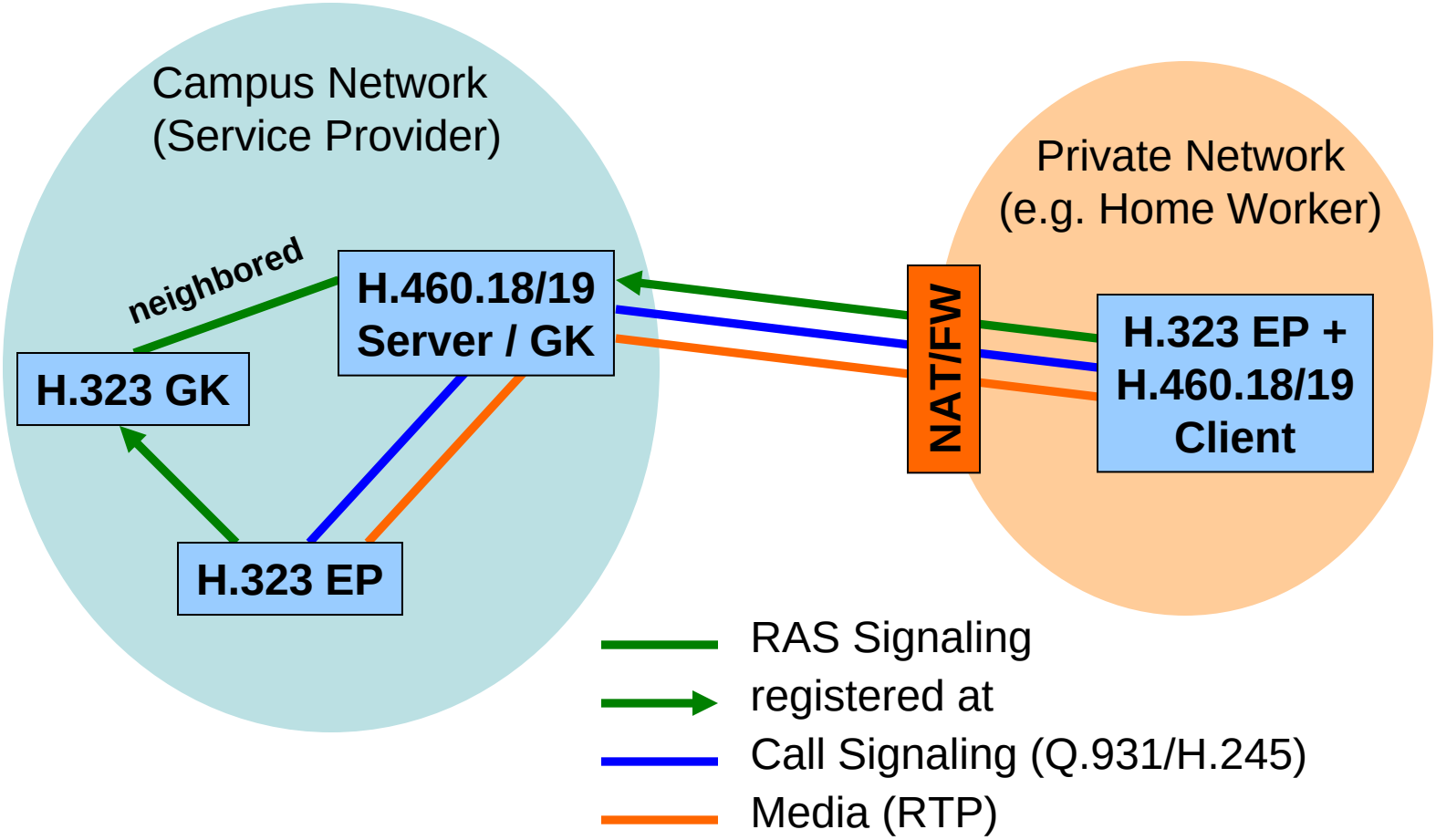
IP header
UDP header
4-byte multiplexID
RTP HEADER
RTP PAYLOAD

General Remarks

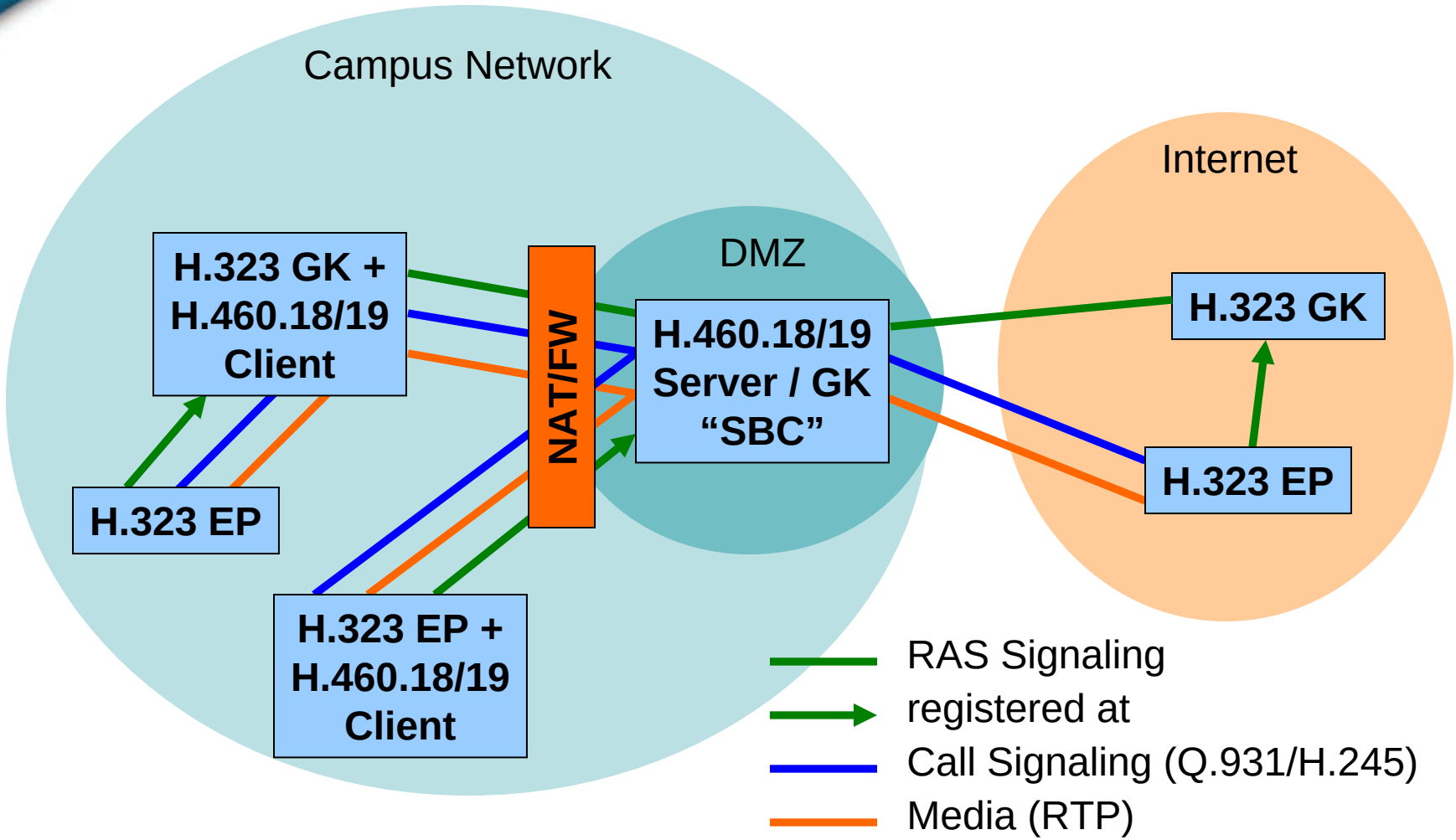
- H.460.18/19 is the accepted standard for H.323 FW/NAT traversal
- Client/Server model, no P2P FW/NAT traversal (like IETF ICE)

- No FW/NAT detection (like IETF STUN)
  → no P2P RTP streams
  → limited scalability

Deployment: Far-end FW/NAT traversal



Deployment: Near-end FW/NAT traversal



Vendor Support

- Tandberg
  - Border Controller = GK + H.460.18/19 Server
  - MXP endpoints include H.460.18/19 Client
- Polycom
  - V2IU servers and VSX endpoints will support H.460.18/19 in Q2/2006
- Radvision
  - PathFinder solution will support H.460.18/19 (Client/Server)
- OpenH323/GnuGK ?
- Interoperability will be an issue

Operational Issues

- H.323-aware NAT/FW or H.323 ALGs do not handle H.460.18/19 correctly
- Cisco PIX “h323 fixup” may interfere with H.460.18/19 call setup (!)
- NAT/FW must allow outgoing TCP/UDP sessions on all high ports

Conclusion

After many years of suffering,
we finally have a standard for H.323
FW/NAT traversal

☺