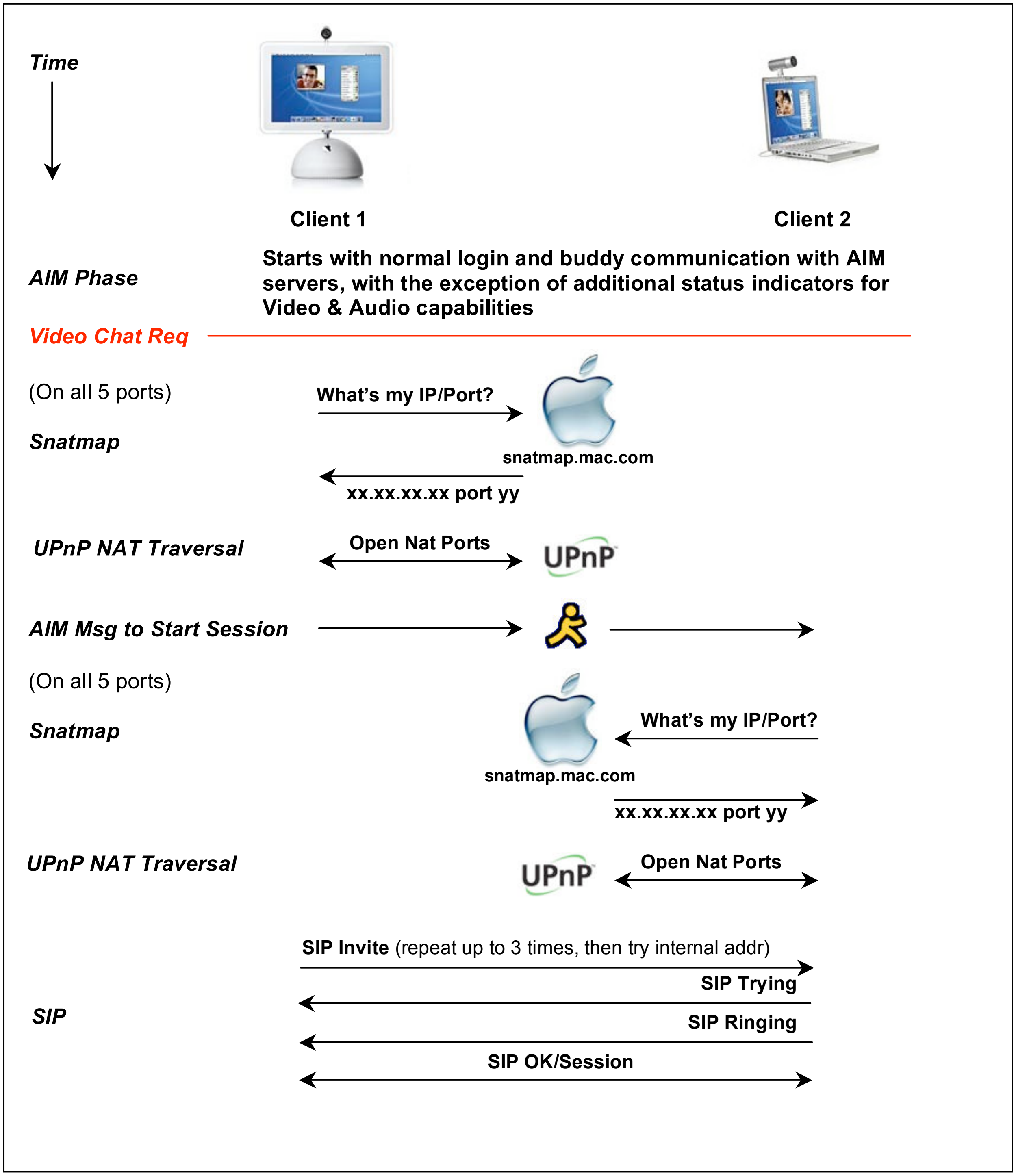
iChat AV Proxy Project

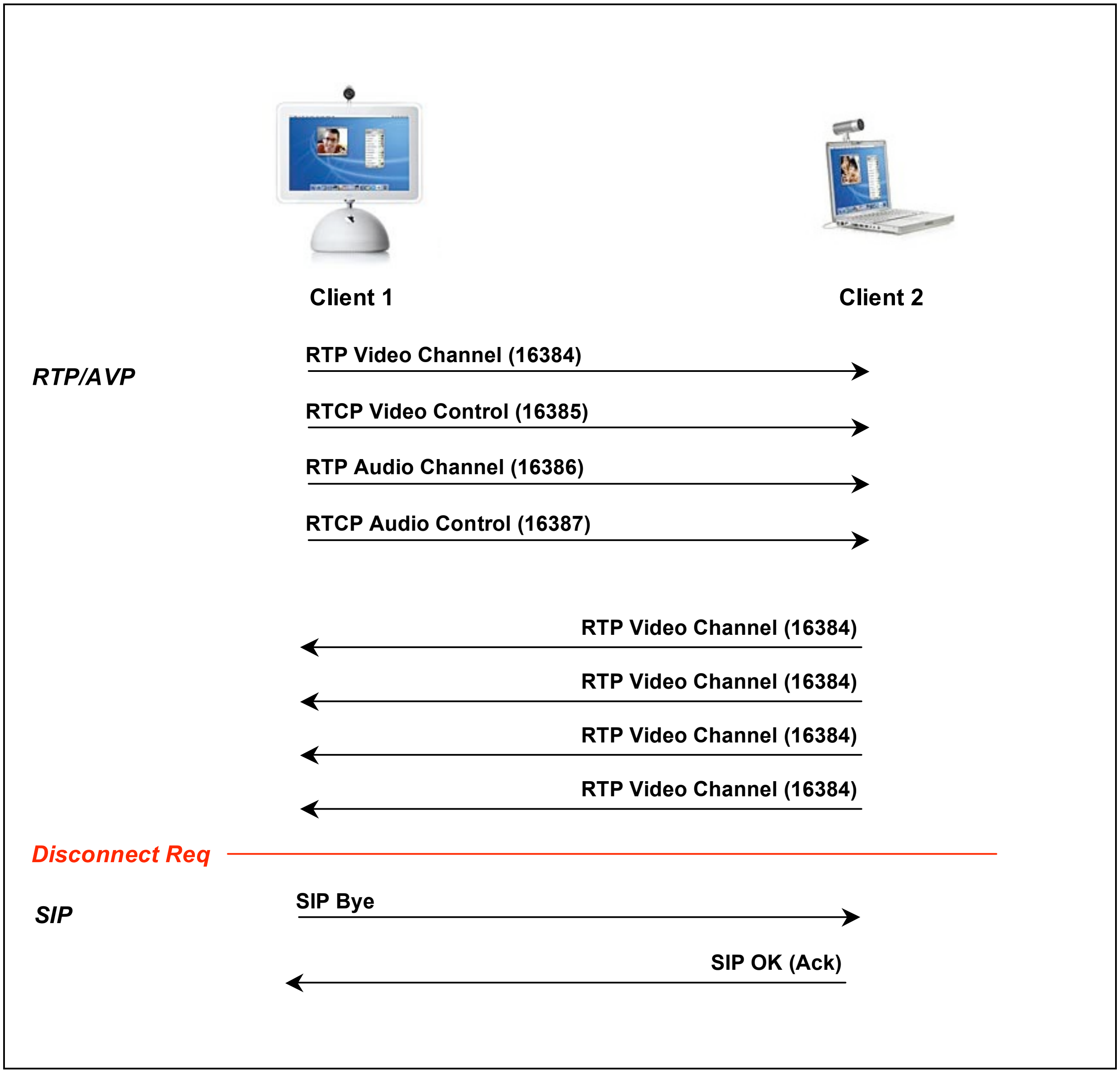
Protocol Overview
Alan Humphherys

Findings

The majority of time this week consisted of reverse engineering and understanding the various protocols used by iChat AV. As a result of this research, I now have a good understanding of which protocols are involved in the sessions. That being said, there are still quite a number of details and vague areas that I still need to investigate and understand. Below is a chart that explains the basics of how iChat AV behaves over time.



Starts with normal login and buddy communication with AIM servers, with the exception of additional status indicators for Video & Audio capabilities


Client 1
Client 2
RTP/AVP
RTP Video Channel (16384)
RTCP Video Control (16385)
RTP Audio Channel (16386)
RTCP Audio Control (16387)
RTP Video Channel (16384)
RTP Video Channel (16384)
RTP Video Channel (16384)
RTP Video Channel (16384)
Disconnect Req
SIP
SIP Bye
SIP OK (Ack)

Protocol Notes:

Snatmap This is a non-published protocol specific to Apple. This protocol serves two purposes, First it allows a client behind a NAT firewall to determine what the external IP address and Port number their internal address/port has been mapped to. The second benefit is that it uses the port in question that has the effect of opening a port mapping back to the client for some types of NAT servers. This is used on all ports that are used in this protocol (5060, 16384, 16385, 16386, 16387)

UPnP (http://www.upnp.org) Although Apple is not an official member of UPnP; they use the NAT traversal mechanism of UPnP to make a request of the NAT router to open a port translation for the requested port. This will work for many new NAT routers out there. When used in conjunction with the Snatmap protocol above, they make best efforts to ensure that at least one of the two ends of the connection has an open port.

SIP iChat uses SIP (Session Initiation Protocol) [*RFC 3261*] to establish the connection directly between the two endpoints without an intervening server. This protocol is used by other multimedia messaging applications (like VoIP) and is a logical choice to be used in this case. SIP is used not only for starting the session but for any muting or exit messages at the end of the session. Traffic on this protocol is bound to port 5060, and cannot move.

RTP The actual audio and video data are sent using RTP (Real Time Protocol) [*RFC 1889*] This protocol is used by most streaming applications in use today. Each end of the stream in iChat uses 4 UDP ports to transmit data. The port numbers used below are the usual numbers used, although they may change. They are specified in the SIP session initiation packets.

Port 16384 – Transmission of Video Stream (using RTP). iChat appears to use H.263 format packets in RTP. At this point the CODEC is unknown.

Port 16385 – Control of Video Stream (using RTCP). These control packets are sent to help establish timing and synchronization of the data stream, as well as give information on packet loss and rate throttling issues.

Port 16386 – Transmission of Audio Stream (using RTP) At this point the CODEC is unknown.

Port 16387 – Control of Audio Stream. (using RTCP). This port appears to be unused, but may be used in some error conditions.