EEG Application Note
iCap™ Networking and Firewall Requirements

Applies to Products: HD480, iCap Captioner PC Software, iCap Broadcast Monitor, ComCC 1250 iCap Hub
Last Revised: November 2011

The iCap™ Realtime Closed Captioning System uses the growing bandwidth and flexibility of today's IP connections to enable a wide range of innovative new features in closed caption authoring, encoding, and monitoring. iCap does this without requiring either broadcasters or caption service providers to open up public IP addresses, VPNs, or port-forwarding tunnels; iCap customers need only a reliable and secure outbound connection to one or more pre-approved trusted server sites. This Application Note describes the networking requirements that do exist for making iCap connections, as well as briefly explaining why iCap, when used properly, provides far better data security than legacy dial-up modem caption systems.

iCap Networking Requirements

All iCap connections are initiated in an outbound direction to a trusted server specified by the operator (or the default configuration files provided by EEG on software installation). In this respect, the iCap software is like a web browser (or other similar program) which can fetch data from places outside your network, but without a need for your PC or caption encoder to be accessible from outside your local network (for example through a globally routable IP address, VPN tunnel, or port forwarding rule). If your firewall does not place restrictions on outbound TCP or UDP connections, you should have no problem operating iCap and no need to change any settings.

Some firewalls do place restrictions on outbound connections, only allowing connections out to a limited "whitelist" of destination IP addresses and/or ports. If this describes your configuration, PCs and caption encoders running iCap will require permission to communicate to the following destinations:

Destination Ports: 9736 (TCP) and 6900 (UDP)
Destination IP Addresses (Required):
64.71.155.195 (California – Fremont)
64.71.155.196
38.117.159.180 (New York – New York City)
Additional Destination IP Addresses (Recommended)
38.117.159.181 (New York - New York City)
173.52.204.20 (New York – Long Island)
216.218.193.139 (California – Fremont)
216.218.193.140

A final consideration is whether your network requires use of proxy servers to make outbound connections. These systems are found mainly in very large-scale IT infrastructures. Support for the SOCKS 5 proxy protocol is currently available in the iCap Captioner and iCap Broadcast Monitor software (from the top toolbar go to **Tools | Options | Proxy Settings**), and is planned for a future release of the iCap Encoder software for HD480. SOCKS 4 is not supported, as it includes no standardized mechanism for handling UDP traffic.

Security Model for Trusted iCap Servers

The iCap service connection software has a built-in Kerberos-style authentication model-your software connects to a server with a known address and sends authentication information encrypted with an iCap public key. After authentication, your client may receive additional encrypted “tickets” which can be used to exchange data with other iCap server locations.

A copy of the iCap public key is included with your iCap software installation. The corresponding private key, required to read your login data and send a response that will be accepted by your software client, is kept secure by EEG and installed only on the selected iCap servers listed above. The complete system guarantees that your client will only send sensitive data once it has received confirmation that the remote server it is contacting is truly an EEG-authorized iCap service point, while also guaranteeing that only an authorized iCap server can access your private login data.

Since all iCap peer clients that you may exchange data with must go through the same authentication protocol, you can be sure that only users who have been authenticated as valid members of groups specifically authorized to do business with you can send data to your iCap clients, or receive data sent by them from your network.

Note on Client Load Balanced Connections

During an iCap session, it is normal for both the encoder and captioner software to make multiple connections to iCap servers – there may be, at one time, a TCP connection to the authentication ticket server, a TCP connection to a “relay” server, and a UDP packet exchange for audio. **As part of the authentication protocol, it is required that all connections associated with a single user session originate from the same IP address.** This is an important consideration if your facility connects to iCap through a load-balanced router system that could dynamically split a single user’s connection requests between multiple paths to the internet. Common symptoms of this problem could include messages indicating that the software has logged in but can not connect to a relay site; or missing audio despite normal caption and chat activity.

To avoid this issue, it is recommended that all iCap traffic from a given section of your local network be directed out preferentially through a single IP address, and only passed to a different router or port if an outage is detected on the primary connection.