EEG Application Note

iCap™ Networking and Firewall Requirements

Applies to Products: HD480/490/491/1490, iCap Captioner PC Software, iCap Broadcast Monitor, ComCC 1250 iCap Hub
Last Revised: March 2015

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.

Outbound Connections Model

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.

If your firewall has a "white-list" allowing outbound connections to only a limited set of IP addresses or ports, see the notes on the next page.

Destination White List

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 and 9744 (TCP) and 6900-6904 (UDP) for standard iCap connections (HD480/490/1490 encoders, PC captioners)

8080 (TCP/HTTP) is also required when synchronizing ComCC systems to the remote iCap server.

Destination IP Addresses

64.71.155.195 (California)
64.71.155.196
216.218.193.139
216.218.193.140
38.117.159.180 (New York)
54.235.150.124 (Virginia)
54.84.222.79
54.85.144.87
54.193.101.112 (California-2)
54.193.41.201
52.11.108.94 (Oregon – iCap BroadcastPlus only)

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**). SOCKS 4 is not supported, as it includes no standardized mechanism for handling UDP traffic.

QoS for iCap Traffic

iCap traffic includes real-time, latency-sensitive audio data that can be much more sensitive to networking issues like packet loss, latency, and jitter than many types of common office traffic like file downloads, email, web browsing, etc. iCap is most similar in requirements to a VoIP phone system; these systems are often placed on a separate network from other office devices, or given QoS priority with the local router. When possible, QoS and isolation are also good ideas for optimizing iCap performance, particularly if you are experiencing problems such as low audio quality, audio re-syncs, or full connection drops.

EEG Support may also be able to help with these problems if you provide your outbound IP address and geographic location. It may be possible to prioritize your account for routing to a local iCap server location that will give you a shorter path than other servers.

Monitoring for iCap

For broadcasters and larger caption agency, EEG strongly recommends setting up monitoring of iCap traffic on your network. Monitoring of bandwidth and availability to iCap server locations can help quickly pinpoint any problems to on-duty staff, and will provide valuable information to EEG Support if the problem appears to be outside of your network. Availability of trace routes and similar logging data makes it much easier to determine whether there are any trouble points on your path to specific iCap server locations.

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.