

Corporate Network Guide for System73 Edge Intelligence (P2P)

Objective: This document provides the technical network requirements for enabling our Edge Intelligence (P2P) technology in scenarios including devices behind corporate networks. These settings apply to all client platforms (web, Android, and iOS) and are necessary for optimal P2P performance. If a P2P connection cannot be established, our service automatically falls back to standard CDN delivery to ensure uninterrupted playback.

1. How It Works

Our technology operates in three main phases to build and run the P2P network:

1. **Signaling and Coordination:** First, the client (whether web or native app) connects to our backend. This is where it learns about other viewers it can potentially connect with.
2. **Connection Establishment (ICE):** Next, it uses the standard **ICE (Interactive Connectivity Establishment)** framework to find the best and most direct connection path to those other peers. This is where STUN servers are used to navigate firewalls.
3. **P2P Data Exchange:** Once a direct link is established, clients begin securely exchanging video segments with each other using the **WebRTC** protocol. This direct peer-to-peer traffic is what reduces the load on your CDN.

The requirements below are designed to ensure all three phases can operate successfully.

2. Network Requirements

For simplicity and to accommodate future service updates, we recommend whitelisting the wildcard domain *.s73cloud.com. If your security policy does not allow wildcards, please use the specific hostnames listed below.

2.1. Backend Communication

- **Recommended:** Allow outbound traffic to *.s73cloud.com
- **Protocol/Port:** [TCP/443](https://) (HTTPS/WSS)
- **Specific Hostnames (if wildcards are not allowed):**
 - **EMEA:** cerberus.emea.polynet.s73cloud.com
 - **Americas:** cerberus.americas.polynet.s73cloud.com

2.2. Peer-to-Peer Connection (ICE Process)

- **Peer Address Discovery (STUN):**
 - **Protocol/Port:** UDP/3478 (Primary), TCP/3478 (Fallback)
 - **Specific Hostnames (if wildcards are not allowed):**
 - **EMEA:** stun-emea-01.s73cloud.com and stun-emea-02.s73cloud.com
 - **Americas:** stun-americas-01.s73cloud.com and stun-americas-02.s73cloud.com
- **P2P Data Exchange (Internal LAN/WLAN):**
 - **Requirement:** Devices must be allowed to communicate directly with each other over local network subnets using UDP with TCP as a fallback.
 - *(Purpose: This is key to reducing your internet bandwidth usage. When users are in the same office, they can share video segments directly without their traffic ever leaving your local network. Please check that any internal firewalls, network access rules (ACLs), or client-side security software don't block this local peer-to-peer traffic.)*
- **NAT Behavior (P2P Compatibility):**
 - The type of Network Address Translation (NAT) implemented by the firewall is a critical factor for enabling direct peer-to-peer connections. For reliable performance, a **Cone NAT** is required.
 - **Why Cone NATs work:** A Cone NAT maps a client's internal IP and port to a single public IP and port. This public mapping is then reusable, allowing inbound packets from *any* peer on the internet to be correctly forwarded to the internal client.
 - **Why Symmetric NAT prevents P2P:** A Symmetric NAT creates a unique mapping for each specific destination. When a client contacts our STUN server, the NAT opens a port that *only accepts return traffic from that STUN server's IP address*. An attempt by a new peer (from a different IP) to connect to that same port will be rejected.
 - *(Note: Our software includes specialized mechanisms to successfully navigate many Symmetric NAT configurations, particularly those that assign ports sequentially. This advanced capability allows Edge Intelligence to establish P2P connections in restrictive environments where other systems would fail. For the most robust performance, a Cone NAT remains the recommended configuration.)*

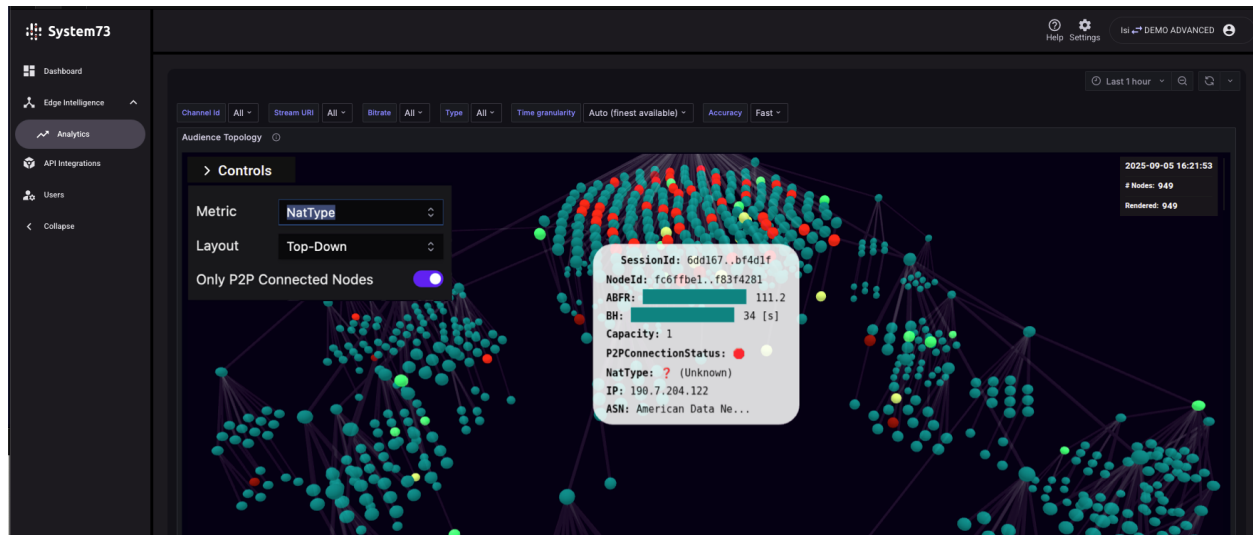
3. Fine-Tuning and Optimization

Beyond the client-side network settings, our platform offers powerful backend configurations to optimize performance for your specific environment.

- **Intelligent Peer Grouping:** The backend can be configured to group users by network identifiers like ASN or ISP. For more granular control, the system can use **custom**

dimensions (e.g., an office ID) provided by your application or player via the integrated Edge Intelligence SDK.

- **Corporate NAT Strategy:** The system's peering logic can be configured for cases where our SDK reports the NAT type as "unknown" for most viewers (see screenshot of System73's analytics dashboard below). Since all users behind the same corporate firewall share a consistent NAT behavior, our system can leverage this to enable P2P connection attempts.



4. Verification Tests

This section provides a suite of tests to validate your network configuration against the requirements.

4.1. Backend Communication Test

From a computer on the corporate network, open a web browser and navigate to the backend URL for your region (i.e. cerberus.emea.polynet.s73cloud.com). A successful connection is indicated by any response other than a browser error like "This site can't be reached." or a timeout. A blank page or a "404 Not Found" error means the test was successful.

4.2. STUN Server Test

This test uses the official WebRTC project's "Trickle ICE" tool to validate STUN connectivity. It validates a client's ability to reach our public STUN servers, which is a key requirement for enabling P2P traffic **between users in different locations over the internet**.

1. **Go to:** <https://webrtc.github.io/test-pages/src/trickle-ice/>
2. **Configure STUN Server:**

- Click **"Remove Server"** to delete the default.
 - In the "STUN or TURN URI" field, enter the address for one of the STUN servers in your region (e.g., `stun:stun-americas-01.s73cloud.com:3478`).
 - Click **"Add Server"**.
3. **Run Test:** Click **"Gather candidates"**.
 4. **Check Results:** In the text box on the right, you should see a candidate with **type srflx** (for UDP) and may also see candidates related to TCP. This confirms your network can reach our STUN server.

Important: While this test is essential for enabling internet-based P2P, it is **not** a hard requirement for achieving P2P traffic *between users within the same corporate LAN*. As mentioned in Section 3, our system can facilitate direct connections using local network addresses even if the NAT type cannot be properly discovered.

4.3. Internal Network Test (LAN/WLAN)

This test confirms that devices on the same local network can communicate directly. For network administrators, the most reliable tool is **iperf3**.

1. **On Device A (Server):** Run `iperf3 -s`.
2. **On Device B (Client):** Run `iperf3 -c <IP address of Device A> -u -b 10M` to test UDP. You can also run it without the `-u` flag to test TCP.
A successful test will show transfer statistics, confirming local communication is working correctly.

5. Recommended Onboarding Approach

While this guide is comprehensive, we find a practical, test-driven approach is often the most efficient path to a successful deployment.

1. **Live Integration Test:** The next step is to conduct a small-scale test using your player integrated with our SDK on a few devices within your corporate network. In many cases, the P2P network will function effectively "out-of-the-box" with just our initial backend changes.
2. **Backend Configuration (if required):** Based on our experience with similar corporate environments, our team could apply a set of proven backend optimizations (as described in Section 3) to your account.
3. **Data-Driven Analysis:** If the test does not yield optimal P2P performance, the metrics reported by our SDK are invaluable. This data allows our team to accurately diagnose the specific bottleneck and provide your networking team with precise, targeted recommendations.

This iterative, data-driven process simplifies onboarding by focusing efforts on confirmed issues rather than hypothetical ones.

6. Document Information

- **Version:** 1.0
- **Creator:** Isi Ramírez / System73
- **Date Created:** September 5, 2025
- **Status:** Final
- **Audience:** Customer IT & Network Administrators