



Hello CAA E-Sports Community,

Ensuring a secure and optimized network environment is essential for successful esports programs in schools. The PlayVS guidance provides a structured approach to network configuration that balances performance with security. By using VLAN segmentation, dedicated public IPs, and strict traffic controls, schools can isolate esports traffic from critical systems, prevent unauthorized access, and comply with regulations like CIPA. This setup not only enhances gameplay performance but also safeguards the broader school network—making it a vital blueprint for IT teams supporting competitive gaming.

### **Act Now: Pre-School Year Implementation Is Critical**

It is *crucial* to implement this network configuration **before the school year begins**. Many of the steps—such as securing IP addresses, configuring NAT policies, and setting up VLANs—require lead time and coordination with your IT support team. Delaying these preparations could result in game connectivity issues, security vulnerabilities, or program delays once the season starts.

To ensure a smooth rollout:

- **Share the attached PlayVS network configuration guide** with your IT staff immediately.
- **Schedule time now** for implementation and testing.
- **Communicate early** with district-level IT or third-party providers to secure any needed public IPs or firewall adjustments.

[Download: PlayVS Guidance - Secure Network Configuration for Esports Games \(PDF\)](#)