# Network Analysis Report for Cyber-Cafe DREAMLAND

## Network Topology

The network diagram for the Cyber-Cafe DREAMLAND shows a complex setup with various devices connected. The network uses a star topology, where all devices are connected to a central node, which in this case is the Cisco ISR4331- AX/K9 Router with IP: 192.168.1.2. This router is the gateway for all devices in the network.

## Connected Devices

The network hosts a variety of devices, including:

Smartphones and Tablets: These devices used by customers and connect to the network wireless.

Samsung Smart TVs: These devices are spread across different areas of the cafe, each with a unique IP address.

Gaming PCs (Hela Gaming PC): These are high-performance computers, used for gaming.

PlayStation 5 consoles: These gaming consoles are also part of the network.

Cash Register (Assur Pos Terminal Windows 11): This device is likely used for billing and inventory management.

Internet Cafe Server (HPE PROLIANT ML30 GEN 11): The Server, manages the client hosts and other network services.

Access Points (Wireless Router TP-Link AX3000): These devices extend the wireless coverage of the network.

Grand stream UCM6308 IP PBX: This Firewall is used for network protection from malicious attacks before they can penetrate the network.

## Security and Scalability Improvements

While the current network setup is robust, there are several ways to improve security and scalability:

Network Segmentation: Implement VLANs to separate traffic from different types of devices. This can enhance security by isolating potential threats to a single segment of the network.

Firewall Configuration: Ensure that the firewall is properly configured to block unnecessary inbound traffic and protect the network from potential threats.

Regular Updates: Keep all devices, especially the router and server, updated with the latest security patches.

Secure Wi-Fi: Implement strong encryption (like WPA3) for the Wi-Fi network to protect against unauthorized access.

Intrusion Detection System (IDS): Implement an IDS to monitor the network for malicious activities or policy violations.

Scalability: For future expansion, consider using more scalable network devices and architectures. For instance, a cloud-based server could provide more flexibility than a traditional server.
Also the use of a second switch would be advisable in the future to assure that better connectivity and expansion.