Gaming Center Hub based on Cisco packet Tracer

M Afnan
Department of Electronics and Communication Engineering
Amrita Vishwa Vidyapeetham
Kollam, India
afnanahmed0847@gmail.com

M Y Ravi Teja
Department of Electronics and Communication Engineering
Amrita Vishwa Vidyapeetham
Kollam, India
raviteja205t@gmail.com

N Vivekananda
Department of Electronics and Communication Engineering
Amrita Vishwa Vidyapeetham
Kollam, India
viveknamani2004@gmail.com

Sai Virasith M
Department of Electronics and Communication Engineering
Amrita Vishwa Vidyapeetham
Kollam, India
virasithm@ieee.org

M Vineeth
Department of Electronics and Communication Engineering
Amrita Vishwa Vidyapeetham
Kollam, India
Vineeth.mahadevu@gmail.com

Aswathy K Nair
Department of Electronics and Communication Engineering
Amrita Vishwa Vidyapeetham
Kollam, India
aswathykn@am.amrita.edu

***Abstract*—This paper summarizes the design, development, and installation of a centralized Gaming Centre Hub that properly balances system availability and billing in a test network setup. The system combines a real-time web-based dashboard with an encrypted configured network with Cisco Packet Tracer. 31 client PCs are interconnected through switches, linked to one router and one server. For preventing any form of unauthorized entry, a single system alone—named as the Admin PC—is authorized to access the admin web portal https://gaming-zone-three.vercel.app/. This configuration is similar to an actual gaming center environment where monitoring and control are of prime importance. By implementing Access Control Lists (ACLs) at the router, HTTP access is only allowed to the Admin PC while allowing internal communication among all client systems. The objective of this project is to increase the efficiency of operations, optimize the management of users, and deliver a scalable base for additional growth in gaming centers and cyber cafés. The simulation not only demonstrates technical networking competencies but also marries web development with planning in physical infrastructure. The outcome is an inexpensive yet secure model that can be repeated or expanded within commercial settings. Rigorous testing proves the system's reliability, security, and user accessibility in a controlled network.**

***Index Terms*—Gaming Hub, Cisco Packet Tracer, Access Control List (ACL), Network Simulation, Centralized Monitoring**

I. Introduction

Over the past few years, the popularity of gaming centers and cyber cafes has increased substantially owing to the demand for collaborative high-performance computing environments. Multiplayer gaming sessions, competitive tournaments, and informal games are hosted by these centers for groups of users. Yet, proper management of such environments poses a number of operational complexities such as monitoring system usage, tracking user sessions, billing automation, and secure administrative access. These tasks are carried out manually in most centers, which creates inefficiencies, possible mistakes, and scalability constraints. This necessitates a streamlined solution that automates control and provides real-time insight into system performance and availability, without compromising on network-level security.

The Gaming Centre Hub project meets these concerns by offering a holistic solution that combines network simulation through Cisco Packet Tracer with a real-time, browser-based management platform. In the simulated setup, 31 client systems are set up in a star topology network, attaching via two switches and a router to a central server. One of these PCs acts as the Admin PC, the only device that is allowed to access the admin dashboard served at https://gaming-zone-three.vercel.app/. This dashboard is a control panel to centrally manage tasks like session management, billing, and viewing each system's availability status. The selective access control is implemented through an Access Control List (ACL) to the router such that only the Admin PC has access to HTTP services on the server.

The prime aim of the project is to present a secure and affordable infrastructure that reflects actual gaming conditions. With the implementation of simulated network elements with a live-deployed web interface, this hybrid platform enables administrators to have complete management over resources while providing secure, trustworthy communication throughout the network. In contrast to conventional configurations that are dependent on proprietary software or loosely integrated systems, this method closely integrates the network infrastructure with administrative services with open-source and available tools. The simulation provides learners, teachers, and developers with a useful learning experience in applying networking concepts based on real-world conditions as well

as demonstrating how web-based technologies can improve centralized administration in a local network setup. With this project, we show how any ordinary gaming center can be upgraded with very little investment in software and hardware facilities.

II. Design and Implementation

A. System Architecture

The Gaming Centre Hub design is based on a star structure which divides client systems effectively through a two-tier switching hierarchy. There are 31 PCs, which are split across two 2960 switches—Switch1 serves 22 PCs, and Switch2 serves the other 9 PCs, including the Admin PC. These switches are interconnected and are connected to a Cisco 2811 router, which is further linked to a Web-Server. Static IP addresses are configured in each client PC from the 192.168.1.0/24 subnet, while the server is in the 192.168.2.0/24 subnet. The router acts as a gateway between the LAN and the server network.

Logical segmentation through IP subnets allows traffic routing and control in an efficient manner. The Admin PC on Switch2 with IP address 192.168.1.31 is the sole device that can access the web dashboard through port 80. This is implemented through an access control list on the FastEthernet0/0 interface of the router. This ACL permits only the IP of the Admin PC to open HTTP sessions to the web server, with all other requests from the LAN being blocked. Internal communication in the LAN is allowed, allowing for uninterrupted gameplay and sharing of files. This design structure maintains security while ensuring usability, offering control centralization without hindering operational flow.

B. Algorithm/Flow Chart

1) Algorithm Description: This algorithm specifies the process to implement a secure network in which only the Admin PC has access to the centralized web application for billing and monitoring the system. .

2) Algorithm Steps and Flow Chart:

- **Start Simulation:** Launch Cisco Packet Tracer and create a new project.
- **Add Devices to Network:** Place 31 PCs, 2 switches, 1 router, and 1 server into the simulation workspace.
- **Assign Static IPs:**
  - Assign each PC a unique IP address in the 192.168.1.0/24 subnet.
  - Assign the server an IP address in the 192.168.2.0/24 subnet (e.g., 192.168.2.10).
- **Configure Router and Server:**
  - Configure router interfaces with appropriate IPs.
  - Enable the HTTP service on the server.
- **Apply ACL to Router:**
  - Create an Access Control List (ACL) that:
    - Permits only the Admin PC (IP: 192.168.1.31) to access the server (IP: 192.168.2.10) on port 80.
    - Denies all other devices from accessing the server.
  - Apply the ACL to the appropriate inbound/outbound router interface.
- **Access Website from PC:** Attempt to access `https://gaming-zone-three.vercel.app/` from any PC.
- **Check Condition:**
  - If PC IP address is `192.168.1.31 (Admin PC)` → Allow HTTP access to the web server.
  - Else → Deny the access request using the ACL.
- **End Simulation**

C. Circuit Diagram

The circuit diagram for the Gaming Centre Hub illustrates the physical and logical connections between network devices, similar to an actual commercial gaming center installation. The 31 PCs are accessed through copper straight-through cables to two switches—Switch1 is used to accommodate PCs 1 through 22, and Switch2 is used to accommodate PCs 23 to 31, including the Admin PC at station 31. There is a direct connection between the switches for inter-switch communication. Both switches are routed through a Cisco 2811 router, which provides communication with the internal LAN and the external server.

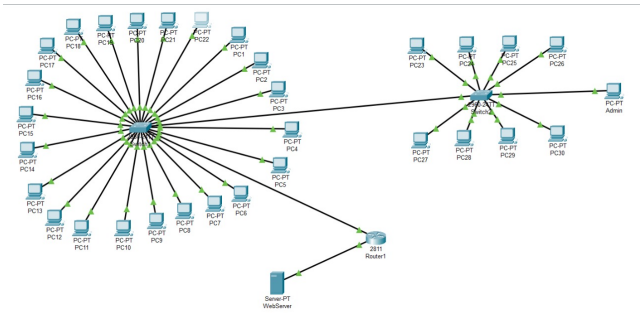

Fig. 1. Circuit Diagram Implemented in Cisco Packet Tracer

The router has two FastEthernet interfaces: FastEthernet0/0 with IP 192.168.1.254 (LAN side) and FastEthernet0/1 with IP 192.168.2.1 (Server side). The server with IP 192.168.2.10 is directly connected to the router and contains the admin dashboard. Router ACLs are used to restrict access to the server so that only 192.168.1.31 (Admin PC) traffic is able to hit port 80. Cables are all assigned to a designated switch port to preserve accuracy. This diagram not only assists in the visualization of data flow but also in the identification of possible points of troubleshooting and confirmation of the physical correctness of the simulated environment.

III. Results

The result of the simulation verifies that the design along with the access control policy is properly implemented. When the Admin PC at IP 192.168.1.31 launches a browser to access https://gaming-zone-three.vercel.app/, the website loads immediately. This confirms that the Access Control List allows HTTP traffic from the Admin PC to the web server. The

interface is responsive and clearly reflects changes in system status and gives a robust, real-time control panel with which to manage the gaming center effectively.

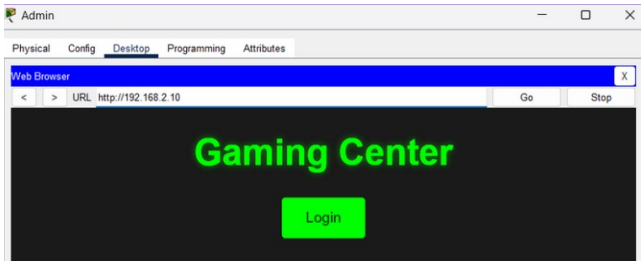

Fig. 2. Admin PC is getting access

With a second and more critical test, any other PC, say PC15 or PC22 other than Admin PC, sends a request to try accessing the same URL. The request is blocked and the browser displays an error or failed connection; thus, the ACL is indeed preventing access from any unauthorized source, but it allows LAN communication among the PCs just as it was. All PCs can now ping each other and share files with no network protocol problems. The simulation shows that selective enforcement of access policies is possible without drastic degradation of overall network services, thus realizing both control and operational continuity.

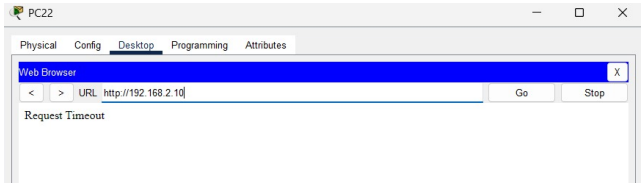

Fig. 3. Non Admin PC is not getting access

Conclusion

The Gaming Centre Hub project well illustrates a safe, centralized administration system for gaming environments through Cisco Packet Tracer and an online web application. Through the restriction of only the Admin PC to access the web portal https://gaming-zone-three.vercel.app/, the project well implements access control through ACLs on a simulated network. Through this, administrative activities such as billing and monitoring are kept safe and segregated from normal client systems. The architecture, with 31 PCs in two switches, a router, and a server, presents a plausible model for a gaming center. The coupling of networking with an active website closes the gap between simulation and actual deployment, illustrating a real-world solution for effective resource usage. Internal LAN features are left intact, and administrative rights are safely limited. This project presents a teachable and scalable system, showcasing how a simple tool and intelligent design can provide high-level control and security in a game center or cyber café with limited infrastructure.

Future Works

The present setup provides a solid platform, but evolving enhancements can take the Gaming Centre Hub to an even more powerful and intelligent system. Adding a database to retain session histories and billing information would enable sophisticated reporting and analytics. Biometric or RFID-based user authentication would simplify user login and automate session monitoring. The web application could be optimized for mobile use, enabling admins to control the hub remotely. The deployment of firewall rules and bandwidth monitoring would further optimize and secure the network. Payment gateway integration can automate postpaid or prepaid session billing for games. Predictive analytics based on machine learning can also optimize resource allocation by predicting peak usage hours. IPv6 support and system health monitoring can stabilize and modernize the configuration for bigger deployments. These future developments would convert the existing system from a secure simulation model to a complete, intelligent gaming center management platform appropriate for real-world commercial operations and schools.