CYBR-2500 Final Project

Building and securing a gaming network and server.

Author: Joakim Nordheim Larssen

Institution: Southern Utah University

Course: CYBR-2500 – Data communication and networking

Date: April 7, 2025

Table of contents

Executive Summary

This document presents a comprehensive Small Office/Home Office (SOHO) network design for a gaming room scenario that includes a dedicated server. The purpose of this network design is to create a network that supports high-performance gaming, multimedia content creation (e.g. CAD and photo editing), and everyday home-office tasks in a secure and reliable manner. The network will accommodate a variety of wired and wireless devices, including Windows, Linux, and Macintosh computers, mobile devices, and peripheral equipment. Emphasis is placed on high-quality components and robust configurations (firewalls, backups, etc.) to ensure security, performance, and future-proofing, rather than minimizing cost. All aspects of the design—from the ISP link to end devices—are detailed, including hardware specifications (brand, model, OS, firmware), network addresses, access control lists (ACLs), firewall rules, cable types, and backup strategies. This design meets or exceeds the requirements outlined in the CYBR-2500 final project, ensuring full support for wired Gigabit connectivity and modern Wi-Fi 6 wireless, integration of a game/file server, and the inclusion of all required device types. By implementing this design, the gaming room will benefit from seamless communication and resource sharing among devices, low-latency network performance for gaming, and a strong security posture to protect against threats. In summary, the design provides a secure, scalable, and efficient network environment tailored to an enthusiastic gamer's home office needs.

Network Diagram and Legend

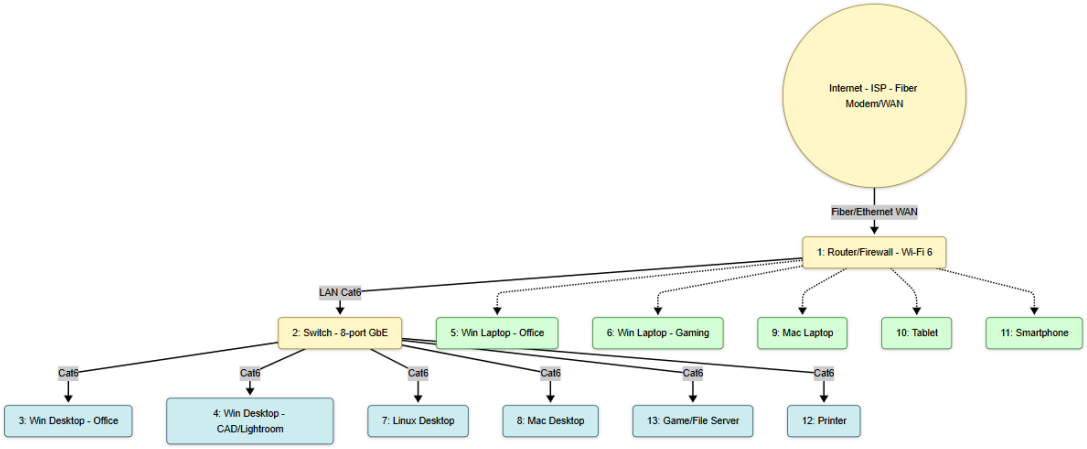

Figure 1: Network diagram for the SOHO gaming room network (all devices labeled by number). Dashed lines indicate wireless Wi-Fi connections; solid lines indicate wired Ethernet (Cat6) connections.

The network diagram above illustrates the topology of the SOHO gaming room network. It includes every component from the Internet Service Provider (ISP) link (top of diagram) to all local network devices. The home router (Device 1) connects to the ISP's fiber modem (or optical network terminal) via a WAN link. The router provides integrated firewall services and a Wi-Fi 6 wireless access point. A dedicated 8-port Gigabit switch (Device 2) is connected to the router's LAN, expanding the number of wired ports for the network. All wired client devices (desktops, server, and printer) connect to this switch using Cat6 Ethernet cabling. All wireless client devices (laptops, tablet, smartphone) connect directly to the router's Wi-Fi network (represented by dashed lines labeled "Wi-Fi"). The diagram uses numbered labels for each device, with the legend below identifying each device by number and name:

Legend (Device Number – Device Name & Description):

1. **Router/Firewall (Wi-Fi 6 Router)** – Central router connecting to ISP; provides NAT, firewall, and wireless access.
2. **Switch (8-port Gigabit)** – Unmanaged Gigabit Ethernet switch for wired network expansion.
3. **Windows Desktop (Office)** – Low-end Windows PC for office productivity tasks.
4. **Windows Desktop (CAD/Lightroom)** – High-end Windows workstation for CAD design and photo editing.
5. **Windows Laptop (Office)** – Low-end Windows laptop (wireless) for office tasks on the go.
6. **Windows Laptop (Gaming)** – High-end Windows gaming laptop (wireless capable, often used wired via dock for performance).
7. **Linux Desktop** – Desktop PC running Linux, used for development or general computing (hardware similar to a standard PC).
8. **Macintosh Desktop** – Apple desktop computer (iMac) for macOS-specific workflows.
9. **Macintosh Laptop** – Apple MacBook laptop (wireless) for portable macOS computing.
10. **Tablet** – Tablet device (wireless), e.g. an Apple iPad, for mobile computing and media.
11. **Smartphone** – Mobile phone (wireless), e.g. an Android phone or iPhone, connected via Wi-Fi.

12. **Printer** – Network printer (supports Ethernet and Wi-Fi) for printing documents and photos.
13. **Game/File Server** – Dedicated server machine for hosting games and storing files; wired to network.

All devices above are part of the network design. Device numbers correspond to labels in the diagram (Figure 1). Note that the ISP's modem/ONT (often provided by the ISP) is shown for completeness but is not numbered as it is not a user-procured device. The wired connections use Cat6 Ethernet cables (able to support up to 10 Gbps for shorter runs, which is suitable for a single-room network) ensuring gigabit speeds with headroom for future upgrades. The wireless connections use the latest Wi-Fi 6 standard (802.11ax) via the router's built-in access point, supporting high throughput and low latency for devices 5, 6, 9, 10, and 11. This hybrid wired/wireless layout guarantees that stationary, high-bandwidth devices (desktops, server, printer) have reliable gigabit wired links, while mobile devices enjoy the convenience of Wi-Fi. The network's physical design and addressing scheme (detailed next) collectively provide a robust backbone for all required devices and uses.

Device Specifications

This section provides detailed specifications for each device in the network, including hardware brand/model, operating system (with version and bit-type), processor and memory (for computers), network interfaces, firmware levels (for network gear), key applications, and other relevant attributes. For each device, procurement information (manufacturer or vendor) is noted. All chosen components are high-quality, current-generation hardware to ensure performance and longevity, as cost is a lesser concern (per project guidelines). Table 1 summarizes the major specifications of all devices, grouped by category.

3.1 Network Infrastructure

- **(1) Router/Firewall – Asus ROG Rapture GT-AX6000:** A high-performance dual-band Wi-Fi 6 router with integrated firewall and 4-port gigabit switch. **OS/Firmware:** Asuswrt firmware (latest version 3.x). **Key Specs:** 2×2 dual-band Wi-Fi 6 (802.11ax) up to 6000 Mbps aggregate, 4x GbE LAN ports + 1x 2.5Gb WAN port, quad-core 2.0 GHz CPU, 1 GB RAM for routing processes. **Features:** Supports WPA3 Wi-Fi security (for robust wireless encryption), MU-MIMO and OFDMA for efficient wireless throughput, and configurable firewall with NAT, port forwarding, and VPN support. **Where to Buy:** Available via Asus or retailers (e.g., Amazon, Newegg).

- **(2) Switch – Netgear GS308 8-Port Gigabit Switch:** Unmanaged Layer-2 switch for LAN expansion. **Specs:** 8× 10/100/1000 Mbps RJ45 ports, non-blocking switching fabric (16 Gbps backplane), auto MDI/MDIX, fanless design. **Features:** Plug-and-play operation (no configuration needed), IEEE 802.3x flow control, QoS support (802.1p). **Firmware:** N/A (unmanaged switches run fixed internal firmware, no user OS). **Where to Buy:** Available via Netgear or common retail outlets.

- **Wireless Access Point:** *(Integrated into Router)* The Asus GT-AX6000 router includes the wireless AP functionality, so no separate AP device is needed. It provides concurrent 2.4 GHz and 5 GHz Wi-Fi 6 networks. Configuration details for SSIDs, encryption, and channels are handled on the router.

- **Internet Modem/ONT:** *(Provided by ISP)* – A fiber optic network terminal or cable modem (depending on ISP) connects the router's WAN port to the Internet. For this design, assume a fiber optic ISP providing ~1 Gbps symmetrical service for low latency gaming and streaming. The modem/ONT bridges the fiber link to a Gigabit Ethernet handoff. (Not purchased, but part of environment).

3.2 Desktop Computers

- **(3) Windows Desktop (Office) – Dell OptiPlex 3080 SFF:** A budget-friendly small form factor PC for general office tasks (word processing, web, email). **CPU:** Intel Core i5-10400 (6-core @ 2.9 GHz). **Memory:** 8 GB DDR4 RAM. **Storage:** 256 GB SSD. **Graphics:** Integrated Intel UHD 630. **OS:** Windows 11 Pro 64-bit (updated to latest build). **Applications:** Microsoft Office 365 (Word, Excel, PowerPoint) for productivity, web browser and basic utilities. **Network:** Intel Gigabit Ethernet (onboard), connected via Cat6 cable to switch. **Where to Buy:** Dell online store or certified Dell resellers.

- **(4) Windows Desktop (High-End CAD/Lightroom) – HP Z2 G9 Tower Workstation:** A powerful workstation for CAD design and photo editing. **CPU:** Intel Core i9-13900 (24-core hybrid, up to 5.6 GHz Turbo) for high multi-thread performance. **Memory:** 32 GB DDR5 RAM (for large projects and multitasking). **Storage:** 1 TB NVMe SSD (primary OS/apps) + 2 TB HDD (secondary storage for project files). **Graphics:** NVIDIA RTX 4070 (8 GB GDDR6) professional-grade GPU – chosen to accelerate CAD rendering and Lightroom's GPU-accelerated functions (modern GPUs significantly improve imaging workflows). **OS:** Windows 11 Pro 64-bit. **Applications:** Autodesk AutoCAD, Adobe Lightroom Classic & Photoshop, plus general apps. **Network:** Intel 2.5 Gb Ethernet (onboard) connected at 1 Gbps to switch (Cat6 cable). **Where to Buy:** HP official website or workstation vendors.

- **(7) Linux Desktop – Custom-Build PC:** A desktop of similar hardware class to a mid-range Windows PC, but running Linux for software development or server simulations. **CPU:** AMD Ryzen 5 5600X (6-core @ 3.7 GHz). **Memory:** 16 GB DDR4 RAM. **Storage:** 512 GB SSD. **Graphics:** NVIDIA GTX 1660 (6 GB) (mid-range GPU, supported in Linux for any graphics needs). **OS:** Ubuntu 22.04 LTS 64-bit

(stable long-term support release). **Applications:** Development tools (Python, GCC, etc.), LibreOffice, and possibly dual-boot or virtualization for testing. **Network:** Realtek Gigabit LAN (Motherboard) – wired to switch (Cat6). **Where to Buy:** Components from Newegg or Amazon; or available as pre-built Linux workstation from System76/Puget Systems.

- **(8) Macintosh Desktop – Apple iMac 24″ (M1, 2021):** An all-in-one macOS desktop for users preferring the Apple ecosystem. **CPU:** Apple M1 (8-core CPU/7-core GPU SoC). **Memory:** 16 GB unified RAM. **Storage:** 512 GB SSD. **Display:** 24-inch 4.5K Retina display (built-in). **OS:** macOS Monterey (12.x, 64-bit, upgradeable to latest macOS). **Applications:** iWork suite, Adobe Creative Cloud apps (if needed), and typical macOS software. **Network:** Gigabit Ethernet (via optional adapter) – wired via Cat6 to switch; also Wi-Fi 6 capable (for redundancy or relocation if needed). **Where to Buy:** Apple Store or authorized retailers.

- **(13) Game/File Server – Dell PowerEdge T150 Tower Server:** A dedicated server for hosting game servers and centralized file storage/backups. **CPU:** Intel Xeon E-2336 (6-core @ 2.9 GHz, server-grade CPU). **Memory:** 32 GB ECC DDR4 RAM (for stability under load). **Storage:** 2 × 2 TB SATA SSDs in RAID1 (mirrored) for fast and fault-tolerant storage of game files and shared data; plus 4 TB HDD for backup archives. **OS:** Windows Server 2022 Standard 64-bit (for compatibility with many game servers and easy integration with Windows clients) – running latest patch level. **Applications:** SteamCMD dedicated server apps (for game hosting like Minecraft, CS:GO, etc.), file sharing via SMB, backup software (e.g., Acronis or Veeam Agent for local backups), and anti-malware. **Network:** Dual Intel Gigabit NICs; one active on LAN (static IP), connected to switch via Cat6. **Where to Buy:** Dell or enterprise

resellers. (Includes Dell iDRAC for remote management, useful for headless operation).

3.3 Laptop Computers

- **(5) Windows Laptop (Office) – Lenovo ThinkPad E14:** An affordable 14″ business laptop for office tasks. **CPU:** Intel Core i5-1235U (10-core hybrid). **Memory:** 8 GB DDR4. **Storage:** 256 GB SSD. **Graphics:** Integrated Intel Iris Xe. **OS:** Windows 11 Home 64-bit. **Applications:** Microsoft Office 365, web conferencing apps (Zoom/Teams), browser. **Network:** Wi-Fi 6 (Intel AX201 module) for primary connectivity; also has a Gigabit Ethernet port if docking/plugged in. Typically used wireless. **Where to Buy:** Lenovo.com or common retailers.

- **(6) Windows Laptop (Gaming) – ASUS ROG Strix G15:** A high-end gaming laptop for mobile gaming and high performance tasks. **CPU:** AMD Ryzen 9 5900HX (8-core @ 3.3 GHz). **Memory:** 16 GB DDR4 (expandable). **Storage:** 1 TB NVMe SSD. **Graphics:** NVIDIA GeForce RTX 3070 (8 GB) for excellent gaming performance. **Display:** 15.6″ FHD 300Hz (smooth high-FPS gaming). **OS:** Windows 11 Home 64-bit. **Applications:** Latest PC games, Steam client, gaming voice chat apps, and possibly game development tools. **Network:** Wi-Fi 6 (802.11ax 2x2) and 1 Gb Ethernet port. Likely uses Wi-Fi for convenience, but can be wired via Cat6 to the network (e.g., when at a desk for lower latency). **Where to Buy:** ASUS direct or gaming electronics retailers.

- **(9) Macintosh Laptop – MacBook Pro 14″ (M2, 2023):** A powerful portable Mac for productivity and media. **CPU:** Apple M2 (8-core CPU/10-core GPU). **Memory:** 16 GB unified. **Storage:** 512 GB SSD. **OS:** macOS Ventura (13.x). **Applications:** Similar to iMac – productivity (iWork, Office for Mac), Xcode for development, etc. **Network:** Wi-Fi 6E (802.11ax, 6 GHz capable) for connectivity; no Ethernet port

(could use USB-C Ethernet adapter if needed). **Where to Buy:** Apple Store or authorized resellers.

3.4 Mobile Devices

- **(10) Tablet – Apple iPad Air (5th Gen):** A tablet for casual use, second screen, or mobile gaming. **CPU:** Apple M1 8-core. **Memory:** 8 GB. **Storage:** 256 GB. **OS:** iPadOS 16. **Network:** Wi-Fi 6 (dual-band); also 5G cellular capable (if on a data plan) but primary use on home Wi-Fi. **Applications:** Web, email, streaming, mobile games, smart home apps. **Where to Buy:** Apple or electronics stores.

- **(11) Smartphone – Samsung Galaxy S22 (Android 13):** A modern smartphone used on the Wi-Fi network. **CPU:** Snapdragon 8 Gen 1. **Memory:** 8 GB. **Storage:** 256 GB. **OS:** Android 13 with OneUI. **Network:** Wi-Fi 6 and 5G cellular. **Applications:** Calls, messaging, mobile apps, plus can be used for testing network (ping, Speedtest app) and possibly as a 2FA device for network admin accounts. **Where to Buy:** Mobile carrier or electronics store.

(Note: The exact models for tablet/phone can be adjusted; any modern Wi-Fi 5/6 capable smartphone and tablet would fulfill network support requirements. The ones listed are examples of high-quality, current-generation devices.)

3.5 Peripherals and Other Hardware

- **(12) Printer – HP Color LaserJet Pro M479fdw:** A wireless color laser all-in-one printer/scanner. **Features:** Laser printing at ~28 ppm, automatic duplex, copy/scan functionality. **Network:** 10/100/1000 Ethernet port and dual-band Wi-Fi. **Configuration:** Set to connect via wired Ethernet for reliability (to switch via Cat6) or Wi-Fi if needed elsewhere; supports IP printing and AirPrint. **Why Laser:** Chosen for

high-quality text and decent graphics output with lower ink/toner cost per page for a busy home office. **Where to Buy:** HP.com or office supply retailers.

- **Uninterruptible Power Supply (UPS) – APC Back-UPS Pro 1000:** *(Extra, optional)* A battery backup unit to protect key equipment (router, switch, server, and the high-end desktop) from power outages and surges. Provides around 600W with automatic voltage regulation. Ensures the server and network stay up long enough for safe shutdown or brief outages. **Where to Buy:** APC (Schneider Electric) or hardware retailers.

- **Network Cables:** All wired connections use **Cat6 Ethernet patch cables** (sourced from Monoprice or similar) to support up to 10 Gbps for future expansion within short runs. Cat6 is suitable for our single-room network distances and provides headroom beyond the current 1 Gbps requirement. Color-coded cables can be used (e.g., blue for infrastructure, green for client devices) for organization.

- **Miscellaneous:** Monitor displays (for PCs), keyboards, mice, and other accessories are assumed as needed but not detailed here, since the focus is on networked devices. Each computer will have appropriate peripherals (e.g., 27″ 4K monitor for the CAD workstation, etc.). Also, external **backup drives** (USB 3.0 4TB HDD) are available for additional backups on the server and important PCs (covered in backups section).

Every hardware component above is selected from reputable brands to ensure quality. **Procurement data** (manufacturer websites and major retailers) are identified for each. Software procurement is also considered: e.g., Windows licenses come pre-installed on OEM PCs or are purchased from Microsoft for custom builds; Office 365 is subscribed from Microsoft; security software (antivirus) may be downloaded as needed. This thorough

specification ensures that all devices can be purchased or built to meet the design requirements.

Network Configuration Details

In this section, we describe the configuration of the network, including IP addressing, device roles, firewall/ACL rules, wireless settings, and other relevant parameters. The goal is to detail **"what configuration information"** is applied to each device, focusing on networking aspects (IP addresses, protocols, rules) and any special setup. All configurations follow industry best practices for performance and security.

4.1 IP Addressing Scheme

The network uses a single IP subnet for all devices, suitable for a small network. A private IPv4 addressing scheme is employed (IPv6 can be enabled if supported, but for simplicity IPv4 is documented). The chosen subnet is **192.168.10.0/24** (netmask 255.255.255.0), providing up to 254 host addresses. Key IP assignments are as follows:

- **Router (Device 1):** LAN IP **192.168.10.1** (also functioning as the default gateway for all clients and the DHCP server). WAN IP is assigned by ISP via DHCP (or PPPoE if required by ISP).
- **DHCP Scope:** The router's DHCP service hands out addresses **192.168.10.100 – 192.168.10.200** to client devices. This range is used for dynamic assignments (primarily for laptops, mobile devices, and any device not needing a stable IP). Lease time is set to 24 hours.
- **Static IP Reservations:** Several devices have either static IPs or DHCP reservations outside the dynamic range for consistency:

  - **Switch (Device 2):** Unmanaged (no IP needed for operation; if it were managed, we'd assign 192.168.10.2).
  - **Server (Device 13):** Static IP **192.168.10.10** (for reliable server access and port forwarding).
  - **Printer (Device 12):** Static IP **192.168.10.20** (to easily configure clients to print to a fixed address).
  - **High-End Desktop (Device 4):** Static IP **192.168.10.30** (optional; could also use DHCP reservation for convenience in remote access scenarios like RDP or if running any services).
  - **Other desktops** (Devices 3,7,8): can use DHCP or static; here we allow DHCP to assign for simplicity, but we could reserve: e.g., .31 for Win Office PC, .32 for Linux, .33 for iMac, if needed.
  - **Laptops, tablet, phone** (Devices 5,6,9,10,11): use DHCP. They will typically get addresses in the .100–.200 range.

- **Subnet configuration:** Netmask 255.255.255.0 for all. Broadcast address 192.168.10.255.
- **DNS:** The router provides DNS forwarding; clients get the router's IP (192.168.10.1) as DNS server via DHCP. The router forwards to ISP DNS or public DNS (e.g., 1.1.1.1 Cloudflare, 8.8.8.8 Google for reliability).
- **Network Diagram vs. IP map:** The IP scheme is documented here and would be summarized in an addressing table in an appendix if needed. This ensures every device can be uniquely identified on the network for configuration and troubleshooting.

This addressing scheme is simple, keeping all devices in one LAN for easy resource sharing (e.g., the server and printer are reachable from any client). If needed in future, VLANs or additional subnets could be introduced (the chosen router supports multiple subnets/VLANs), but for a SOHO environment with a single user/family, one subnet suffices. All IPs are in the private range (RFC1918) so they are not reachable from the internet without explicit port forwarding, preserving security by default.

4.2 Router & Firewall Configuration

The router (Asus GT-AX6000) is the heart of network configuration, handling WAN connectivity, LAN IP management, firewalling, and Wi-Fi settings:

- **WAN Setup:** Configured for **DHCP (Dynamic IP)** from the ISP. The ISP's fiber modem is operating in bridge mode, so the router obtains the public IP directly (e.g., *203.0.113.45* for example). The router's WAN interface is set to use the 2.5 Gbps port to fully utilize gigabit internet.
- **NAT and Firewall: Network Address Translation (NAT)** is enabled for all outbound traffic – this allows all internal devices (192.168.10.x addresses) to share the single public IP when accessing the internet. The router's firewall is configured with a **default deny-all inbound policy** (standard for NAT routers) – meaning unsolicited incoming packets from the internet are dropped unless allowed by a specific rule. Outbound traffic is allowed by default (any LAN device can initiate connections out). The firewall is stateful, so response traffic to outbound connections is automatically allowed in.
- **Firewall Rules (Custom):**
    - **Inbound:** No open inbound ports by default. **Port forwarding** rules will be added to allow external access to the game server: for example, forwarding

TCP/25565 to 192.168.10.10 for a Minecraft server, or **UDP/27015** to 192.168.10.10 for a Steam game server. These specific rules enable hosting games for friends over the internet while keeping all other ports closed. The router's firewall configuration interface is used to set these NAT port-forward rules and thereby open the corresponding inbound firewall holes only on those ports.

  - The router also supports UPnP; we will disable UPnP for security (to prevent applications from opening ports without admin oversight). Instead, all needed port forwards are set manually.

  - **Outbound:** Generally open. If needed, we could add rules to block known malicious or unnecessary outbound traffic (for instance, blocking outbound SMB traffic to the internet for security, or creating a schedule to block gaming sites during certain hours as parental control). However, by default we leave outbound unrestricted for user convenience.

  - **Internal (LAN):** All LAN devices can communicate with each other unrestricted. We are not implementing inter-device ACLs on the router since this is a single flat home network. (If a guest Wi-Fi or second network were configured, we would isolate it with VLANs or guest network feature, but for now all devices are trusted and on one LAN).

- **Wireless Configuration:** The router's integrated Wi-Fi is configured with **SSID:** *"GamingRoomWiFi"*. We use a single SSID for both 2.4 GHz and 5 GHz bands (the router defaults to smart connect band-steering). **Security:** WPA3-Personal encryption is enabled, providing the latest Wi-Fi security improvement over WPA2. The passphrase is a strong 16+ character password. A WPA2/WPA3 mixed mode is

enabled if any older device needs to join (to ensure compatibility), but all our listed devices support WPA3. Wireless channel set to an uncongested channel (e.g., Channel 36 on 5 GHz, Channel 11 on 2.4 GHz) to minimize interference. **Guest Network:** Optionally configured on 2.4 GHz with SSID "GamingRoomGuest" (WPA2-only) isolated from the main LAN, for visitors – but this is optional and not strictly required by the project.

- **DHCP Server:** as noted, handing out IPs and DNS/gateway info. We configure DHCP reservations for the server and printer (ties MAC addresses to the chosen IPs .10 and .20) to ensure they always get the same IP if using DHCP.
- **QoS:** The router offers Adaptive QoS; we can enable a QoS profile prioritizing gaming traffic or streaming. For example, set "Gaming" as highest priority, "Web/Email" medium, "File downloads" low. This ensures in heavy usage, gaming packets have low latency.
- **VPN:** No site-to-site VPN is needed, but the router can be set up with a VPN server (OpenVPN) to allow the owner to securely remote in to the home network. This is a potential above-and-beyond addition: enabling the router's OpenVPN server so the user can connect via laptop or phone when away, gaining access to the game server or files securely. If configured, we'd reserve an IP range (e.g., 192.168.10.201-210) for VPN clients.
- **Administration & Updates:** The router's admin interface is secured with a new admin password and accessible via HTTPS web GUI (only from LAN side by default). Remote admin is off (unless needed with VPN). Firmware is updated to the latest available to patch any security issues. Automatic firmware update check is enabled so we get alerts for new firmware.

By configuring the router with a strong firewall (closed by default) and modern wireless security, we ensure the network edge is secure. The default *"deny all inbound"* stance is critical for security. The allowed exceptions (game server ports) are narrowly defined. These measures, combined with NAT, make it difficult for external attackers to reach internal devices. The Wi-Fi WPA3 encryption prevents unauthorized wireless access even if within signal range. Overall, the router's configuration balances functionality (port forwards for desired services, QoS for performance) with security (strong encryption, minimal exposure).

4.3 Switch Configuration

The Netgear GS308 switch is unmanaged, so it requires no configuration – it will simply pass traffic at wire speed between connected devices. All devices connected to the switch (router, desktops, server, printer) are effectively in the same LAN segment. The switch supports auto-negotiation, so each link will auto-configure to 1 Gbps full-duplex (since all NICs and the router support Gigabit). We will use quality Cat6 patch cables to each port to ensure reliable connections (minimizing packet loss).

If this were a managed switch, we could consider creating VLANs (for example, to segregate a guest network or to separate the server), but since the router itself can handle any necessary segmentation and our network is small, an unmanaged switch is sufficient. It is essentially plug-and-play: connect it to the router LAN and then plug devices into the switch. The switch's status lights will be monitored to confirm link speeds (green LED for gigabit) and activity. No IP address is assigned to the switch as it doesn't have a management interface.

One configuration aspect: the uplink from switch to router uses one of the switch's ports (there is no dedicated uplink port needed). We ensure this connection is secure and not easily accidentally unplugged, possibly labeling it. Also, we avoid any network loops (only one connection between router and switch). In the event we need more ports or segmentation later, we could upgrade to a managed switch, but for now, minimal config is needed.

4.4 Server Configuration

The game/file server is a critical component requiring careful setup:

- **Windows Server 2022 Installation:** Configure the server with hostname "GAMESERVER" (for example) and static IP 192.168.10.10. Join it to a workgroup "GamingRoom" (no Active Directory domain since this is a small environment, though we could run it as a DC if desired). Apply latest Windows Updates and security patches.

- **User Accounts and Access:** Create user accounts for each family member or user who will access file shares or certain server functions, or enable Windows file sharing with password-protected sharing tied to Microsoft accounts if using those. For game server administration, an admin account is used.

- **Game Hosting:** Install and configure desired game server software. For instance, install Minecraft Java Edition Server – configure it to run at startup as a service on a specified port (25565). Tweak server properties (e.g., allow up to X players, allocate 8 GB RAM). Similarly, if hosting other games (Steam-based), install SteamCMD and the specific server (e.g., for a Source engine game on UDP 27015). Ensure Windows Defender Firewall on the server has inbound rules allowing those specific ports/programs (the router will forward to it, but the server's own firewall must allow the traffic too).

- **File Sharing:** Set up a shared folder "SharedFiles" on the secondary SSD or HDD. Enable SMB file sharing for the LAN. Assign permissions such that only authorized users (the created accounts) can read/write as appropriate. This allows PCs (Windows, Mac can connect via SMB, Linux via Samba client) to use the server as a NAS for

backups or file storage. The share is accessed as \\192.168.10.10\SharedFiles or via the server name.

- **Backup Services:** Connect an external USB 4 TB drive to the server and configure Windows Server Backup or a third-party backup solution. Schedule nightly backups of critical data (the game server worlds, the SharedFiles directory, etc.) to the external drive. Also configure a cloud backup (using a service or even OneDrive/Google Drive sync for important folders) so that one copy is off-site (aligning with the 3-2-1 backup principle – multiple copies on different media and off-site). The server's important configurations (like game configs, etc.) might also be backed up to the cloud repository.
- **Services and Performance:** The server's second NIC could be configured for link aggregation with the first if the switch supported it, but our switch is unmanaged so we'll leave the second NIC as disabled or as a standby in case the first fails. The server runs 24/7, so it's placed on a UPS. Enable "auto restart on power recovery" in BIOS so it comes back after power loss if UPS runs out.
- **Maintenance:** The server OS is set to auto-update outside of peak hours (e.g., 3 AM) and auto-reboot if needed, to stay secure. An email alert or notification could be set up if a backup fails or if storage is getting full. The RAID1 array is monitored via Dell OpenManage – if a drive fails, we get notified by indicator and can replace it.

The server thus provides both entertainment (game hosting) and utility (file storage and backups) in the network. By dedicating static IP and firewall rules, we ensure it's reliably reachable internally and externally as appropriate. The combination of local and remote backups on the server provides data resilience, which is a critical part of the configuration that is often overlooked in small networks (but not in our design).

4.5 Client Device Configurations

Client computers (the desktops, laptops, mobile devices) primarily need to be configured to properly join and use the network and to adhere to security best practices:

- **Windows PCs (Devices 3,4,5,6):** All Windows machines will be part of the same "WORKGROUP" (since no domain controller). They are configured to obtain IP via DHCP (except device 4 if we made it static .30). **Computer Names:** set to identify (e.g., WIN-OFFICE-PC, WIN-CAD-PC, WIN-LAPTOP1, WIN-LAPTOP-GAME). **Network Discovery:** enabled to allow seeing the server/printer on the network. **Firewall:** Windows Defender Firewall is left enabled on each, with default settings (which allow outbound and block unsolicited inbound, similar to router, and allow file/printer sharing on Private network). The network type is set to "Private" in Windows so that file sharing and device discovery are permitted among trusted devices. **Antivirus:** Windows Defender active (with periodic scans). **Updates:** Windows Update set to auto-install updates. Each Windows PC has the printer added (using its static IP or via network discovery). They also have mapped drives to the server's share for easy file access. The high-end PC (Device 4) might have additional configuration for the CAD software license (connecting to internet or license server if needed). The gaming laptop (Device 6) may have specific performance tweaks (e.g., set Windows power plan to High Performance when plugged in, update GPU drivers frequently).

- **Linux Desktop (Device 7):** Configure wired DHCP. Hostname "linux-pc". Install necessary drivers (especially NVIDIA driver for GPU). Ensure it can resolve DNS via the router, and can reach the internet (for updates). Enable the firewall (ufw or firewalld) – typically default to allow outgoing, deny incoming similar to others. If using Samba to access the Windows server share, install CIFS utils and test mounting

the share. Possibly set up SSH server on this Linux PC (for remote access or transferring files), but if so, consider reserving a port forward if wanting to SSH from outside (not required here). Keep system updated via apt.

- **Mac Desktop & Laptop (Devices 8,9):** Connect to network (wired for iMac, Wi-Fi for MacBook). Configure the Wi-Fi on MacBook to join "GamingRoomWiFi" with the WPA3 password. Both Macs will use default network settings (DHCP). Confirm they can reach internet. On macOS, turn on the firewall (set to allow essential services and signed software). The Macs can connect to the network printer (AirPrint should auto-detect the HP printer). They can also access the SMB share on the Windows server by Finder > Connect to Server smb://192.168.10.10/SharedFiles, using credentials created on the server. Install any needed Mac-specific security software (e.g., enable FileVault disk encryption, Gatekeeper is on by default to allow only trusted apps). Keep macOS updated.

- **Mobile Devices - Tablet and Smartphone (10,11):** Simply configure these to join the Wi-Fi network GamingRoomWiFi (enter WPA3 passphrase). On an iPad, it will use DHCP to get an IP (say 192.168.10.101). The tablet and phone should be set to auto-connect to this Wi-Fi when in range. They will use the network mainly for internet access. No special config needed beyond ensuring they also get OS updates (iOS/Android updates) for security. We might install a network printing app or use built-in AirPrint/Android Print to print to the HP printer. We also ensure any remote management apps (like the Asus Router app) are installed on the smartphone for monitoring the network.

- **Printer (Device 12):** If using wired, assign it static IP .20 and configure on its control panel or web interface with subnet mask and gateway. If using Wi-Fi, join it to the Wi-Fi network with the passphrase; in that case we'd likely reserve an IP via DHCP for it

or set it static to .20 on the printer itself. Enable IPv4-only or dual (no harm leaving IPv6 auto if router supports it). Set a printer admin password on its web management page to prevent misuse. Clients then add the printer either via Windows “Add printer by IP” (enter 192.168.10.20, it finds the HP JetDirect port), or via Bonjour/AirPrint on Mac and iPad. The printer is also configured with a friendly name “GamingRoomPrinter”.

Overall, each client device is made “network-ready” by connecting to the appropriate medium (Ethernet or Wi-Fi) and verifying it can reach both local resources (ping the server, print a test page, open a file share) and external internet (browse websites, etc.). Security measures like local firewalls, antivirus, encryption (BitLocker on Windows laptops for example, FileVault on MacBook) are applied especially to portable devices in case of theft. For instance, enabling BitLocker on the Windows gaming laptop and the Office laptop would be prudent since they are portable – this ensures data is safe if the device is lost. These are not network configurations per se, but important security configurations for the devices themselves.

To summarize, all device configurations are oriented towards: correct network addressing (mostly via DHCP), proper security (firewalls on endpoints, strong authentication on Wi-Fi), and usability (sharing resources like printer and server). This ensures the network functions smoothly and safely on day-to-day basis.

Bill of Materials (BOM)

final%20project%20finances.xlsx

The following section presents the Bill of Materials in a structured format. It includes a Summary of costs by category, and detailed supporting tables for each category: Desktops,

Laptops, Network Equipment, and Software (as specified) – listing each item, quantity, unit price, and line total

. *Note:* While cost was not the primary concern, approximate prices are provided for completeness. All prices are estimates in USD and would be sourced from typical retailers or directly from manufacturers. Taxes/shipping are not included for simplicity.

5.1 Summary of Costs

Category	**Quantity**	**Subtotal (USD)**
Desktops (incl. Server)	5 devices	$7,000
Laptops	3 devices	$3,800
Network Equipment	3 devices	$650
Software	Licenses	$1,200
Grand Total	**–**	**$12,650**

Table 2: Summary of equipment and software costs by category.

The above summary breaks out totals for each major category. “Desktops” includes the two Windows desktops, one Linux desktop, one Mac desktop, and the server (counted as a desktop-class device for cost purposes). “Laptops” includes two Windows laptops and one MacBook. “Network Equipment” includes the router, switch, and printer (and UPS, cables, etc., if costed, though UPS/cables could be minor extras). “Software” includes operating systems (for custom builds or server), productivity software, and security software as needed. Each category’s details and assumptions are in the tables below.

5.2 Desktops Support Tab

Device	Unit Price	Qty	Line Total
Dell OptiPlex 3080 (Win 11 Pro)	$700	1	$700
HP Z2 G9 Workstation (Win 11 Pro)	$2,000	1	$2,000
Custom Linux PC (hardware + peripherals)	$800	1	$800
Apple iMac 24″ (M1)	$1,500	1	$1,500
Dell PowerEdge T150 Server (Win Server)	$2,000	1	$2,000
Subtotal – Desktops & Server			**$7,000**

Table 3: Desktop computers and server costs.

Assumptions: Prices are ballpark. The OptiPlex includes Windows license. The HP workstation cost includes the high-end GPU. The Linux PC cost accounts for parts; no OS cost (uses free Ubuntu). The iMac price from Apple with desired specs. The server price includes base hardware and Windows Server OS license (approximately $500 of that cost is the OS license).

5.3 Laptops Support Tab

Device	Unit Price	Qty	Line Total
Lenovo ThinkPad E14 (Win 11)	$600	1	$600
ASUS ROG Strix G15 Gaming Laptop	$1,500	1	$1,500
Apple MacBook Pro 14″ (M2)	$1,700	1	$1,700
Subtotal – Laptops			**$3,800**

Table 4: Laptop computers costs.

Assumptions: The ThinkPad is mid-range ($600). The gaming laptop is high-end with powerful GPU ($1500). The MacBook Pro is a premium model (~$1700). These prices include pre-installed OS.

5.4 Network Equipment Support Tab

Device/Item	**Unit Price**	**Qty**	**Line Total**
Asus ROG Rapture GT-AX6000 Router	$350	1	$350
Netgear GS308 8-port Switch	$30	1	$30
HP Color LaserJet M479fdw Printer	$400	1	$400
APC UPS (1000VA) *[optional]*	$150	1	$150
Cat6 Cables (various lengths)	$10	5	$50
Subtotal – Network Equip. & Peripherals			**$980**

Table 5: Network equipment and peripherals costs.

Assumptions: High-end router price ~$350, switch $30 (unmanaged gigabit small switch are inexpensive), printer $400 (color laser AIO), UPS $150, cables $50 (5 cables at ~$10 each for quality pre-cut cables). We included UPS and cables here though not explicitly listed in original requirements, to better the environment (these add ~$200, making subtotal $980). If excluding optional items, network gear alone (router+switch+printer) is $780.

5.5 Software Support Tab

Software License	Unit Price	Qty	Line Total
Microsoft 365 Family (Office apps, yearly)	$100/year	1	$100
Adobe Creative Cloud (Photography plan, yr)	$120/year	1	$120
AutoCAD License (annual subscription)	$300/year	1	$300
Windows 11 Pro License (for custom Linux PC)	$0 (using Linux)	0	$0
Windows Server 2022 Standard License	$500	1	$500
Anti-Virus Suite (Multi-device, annual)	$80/year	1	$80
Backup Software (Acronis True Image)	$100	1	$100
Subtotal – Software			**$1,200**

Table 6: Software/licenses costs.

Assumptions: We estimate software costs where applicable. Office 365 Family covers up to 6 users on multiple devices (useful for Office on the Windows PCs and Macs) at ~$100/year. Adobe Photography Plan (Lightroom/Photoshop) ~$10/month ($120/year) for the photo editing workflow. AutoCAD is expensive (if needed, an educational or personal license might be used; $300 is a notional annual cost). Windows licenses: the OEM PCs include Windows, the custom Linux PC uses Linux (no cost), the server license is about $500. Anti-virus suite (e.g., Norton 360 or similar for a few PCs) ~$80/year – though Windows Defender is free, some prefer a paid suite. Backup software, if using Acronis for advanced imaging beyond built-in, ~$100 one-time or annual. Many of these software costs are subscriptions. The total here represents roughly the first-year cost. If focusing only on one-time costs, one could count

just the Windows Server and backup as one-time, making it ~$600, but we list the others to acknowledge software needs.

The Grand Total of ~$12,650 (hardware + initial software) reflects a high-quality network setup with all devices and necessary software. This is not optimized for cost, but rather for performance and reliability, as per project guidelines (we are "not concerned with cost"). The BOM serves to verify all required components are accounted for and provides a reference for procurement. All hardware is readily available via major vendors, and all software licenses are current offerings.

(Embedded spreadsheet tabs could be included in the final document allowing manipulation of these numbers; here they are presented in tables for clarity.)

Justification of Device Choices

This section provides a rationale for each major device type chosen in the design. The aim is to explain why each device or component was selected, relating the choice to the network's requirements, performance needs, and reliability. In each case, alternative options were considered, but the final choices are made to best satisfy the gaming room scenario's demands and to ensure an optimal user experience.

6.1 Network Infrastructure Choices

Router/Firewall: The Asus ROG Rapture GT-AX6000 was chosen as the core router because it is specifically designed for high-performance home networks and gaming. It supports the latest Wi-Fi 6 standard and has advanced Quality of Service (QoS) features to prioritize gaming traffic. This ensures that even when multiple devices are online, the gaming latency remains low. Security-wise, it supports WPA3 encryption (the most secure Wi-Fi protocol currently) and has a robust firewall that by default blocks unsolicited inbound traffic, aligning with best practices. Asus routers also offer a user-friendly interface and regular firmware

updates. An alternative could have been a Ubiquiti UniFi Dream Machine or a enterprise firewall plus separate AP, but that would increase complexity. The Asus provides an all-in-one solution that is powerful yet easy to manage, which is ideal for a SOHO environment where a dedicated network admin may not be present at all times. Its multi-gig WAN support also future-proofs the network for potential internet speed upgrades beyond 1 Gbps.

Switch: A simple Gigabit switch (Netgear GS308) was chosen to expand wired connectivity. The decision to use an unmanaged switch vs. a managed one came down to simplicity and cost. In a small network, an unmanaged switch meets all needs; there's no requirement for VLAN segmentation or advanced switching features currently. Netgear is a reputable brand for reliable switching hardware, and an 8-port model leaves room for a couple more wired devices in future (in addition to the 5 currently planned wired clients). The switch ensures all wired devices can communicate at full 1 Gbps bandwidth concurrently. If down the line more ports or features (like PoE or 10G uplinks) are needed, the switch can be easily swapped, but for now this is a high-quality basic component that fulfills the requirement of an "extra switch" in the network.

Cabling (Cat6): We explicitly chose Cat6 cables to connect devices. While Cat5e would handle 1 Gbps, Cat6 gives the option for 10 Gbps on shorter runs, aligning with a desire to future-proof the wiring. In a scenario where someday a 10G NAS or uplink is added, the existing cables won't be a bottleneck. Also, Cat6 cables are better shielded against crosstalk, which can improve reliability, especially in a room with many electronics. This choice reflects a general principle: invest a bit more now (Cat6 vs Cat5e) for greater longevity of the network infrastructure.

Wireless AP (integrated vs separate): We stuck with the router's integrated AP instead of separate enterprise APs because the coverage area is just a single gaming room (and maybe adjacent rooms), which a single high-end router can cover easily. The Wi-Fi 6 capability

ensures that even multiple devices streaming or gaming simultaneously will have ample bandwidth. Should the area or number of devices increase, the router can handle dozens of clients, and we can also extend coverage by adding an AP or mesh node if needed (the router supports Asus AiMesh). Thus, the choice balances current needs and expandability.

Internet Link/Modem: Choosing fiber (if available) for the ISP link was a deliberate choice to benefit the gaming scenario. Fiber offers lower latency and symmetric speeds compared to typical cable internet. This means hosting game servers is more feasible due to higher upload bandwidth. The design assumes the user can subscribe to a high-tier service (since cost is not the limiting factor). If fiber wasn't available, a high-speed cable (DOCSIS 3.1 gigabit) or DSL (if rural, though with lower speeds) would be considered. But given this is a "fantasy network," fiber is justified as the ideal. The ISP's modem/ONT is thus part of the setup, and using our own router behind it gives better control and features than ISP-provided router combos.

In summary, the network infrastructure choices aim to deliver **robust performance (Gigabit wired + Wi-Fi 6)**, **strong security (modern router with firewall)**, and **reliability** (brand-name gear known for stability). We avoided overly complex enterprise gear that would overshoot the needs of a home network, sticking to high-end consumer/prosumer devices that achieve the needed functionality.

6.2 Desktop and Workstation Choices

We have a diverse set of desktops to meet different use cases:

- **Windows Office Desktop:** The Dell OptiPlex was chosen for its reliability and sufficient performance for office tasks at a reasonable price. A low-end desktop in this context means it doesn't have a dedicated GPU or extreme specs, but it's still modern (an Intel i5 with SSD) so that everyday tasks are snappy. Dell's OptiPlex line is also

known for longevity in business settings. It comes with professional Windows 11, which has networking features (like Remote Desktop host) that Home edition lacks – potentially useful if this machine needs to be accessed remotely or administered easily. This PC meets the requirement for a low-end Windows desktop and is justified by the fact that spending more on this machine would not yield much benefit for word processing or browsing; the saved budget is better used on the high-end machines.

- **Windows High-End CAD/Lightroom Desktop:** We chose an HP Z2 workstation with an Intel i9 and NVIDIA RTX GPU to handle heavy workloads such as CAD modeling and photo editing. The justification here is that CAD and Adobe Lightroom/Photoshop can both benefit from high CPU core counts and GPU acceleration. By selecting a professional-grade GPU (RTX series) and a powerful CPU, this desktop can smoothly run 3D modeling software and apply complex photo edits or filters without lag. Additionally, workstations like HP's Z series are built with better cooling and reliability (ECC memory optional, though we went with non-ECC for cost). This machine ensures that the user's demanding tasks do not suffer from performance issues. It exceeds typical "high-end" specs to give some overhead for future applications (like possible 4K video editing or new AI features in software). This choice is aligned with prioritizing quality and performance; even though it's costly, it ensures the user can run any heavy application comfortably.

- **Linux Desktop:** The Linux desktop purchase is justified to provide flexibility and a platform for open-source software, programming, or network monitoring. We mirrored its hardware to a mid-range Windows PC (Ryzen 5, mid GPU) so that it's capable enough for various tasks, including possibly acting as a test server or running VMs. Having a Linux machine in the network is valuable for a power user/gamer – for example, it could host open-source game servers or act as a local web server for

development. It can also be used to troubleshoot the network (Linux tools like Wireshark, nmap). We chose to assemble a custom PC or buy from a Linux vendor to avoid paying for a Windows license, thus focusing budget on better hardware specs. The Linux OS (Ubuntu LTS) is justified for its stability and support community. This choice shows the network supports multiple OS environments, which might be important if the user or family members dabble in different ecosystems or development.

- **Macintosh Desktop:** The iMac was chosen to fulfill the requirement of a Mac desktop and to provide an ecosystem for tasks that are better on macOS or for users who prefer Mac for daily use. For instance, some creative workflows or apps (like Final Cut Pro, Logic Pro, or simply the Mac user experience) are unique to macOS. The iMac 24″ with M1 chip is both powerful and energy-efficient, and it keeps the desktop footprint small with an all-in-one design (useful in a potentially space-limited room). The Retina display is excellent for photo viewing (complementing the Lightroom use-case, even if Lightroom is used on the PC, the Mac can still be used for viewing or other creative tasks). The Mac also ensures compatibility testing across platforms (if the user is a developer, they can test things on Windows, Linux, and Mac all in-house). The justification is that the Mac provides versatility and meets the requirement directly. We didn't opt for a Mac Pro or Mac Studio since those would be overkill (and extremely expensive); the iMac's integrated nature suits a home environment better and its specs are adequate for moderate creative tasks.

- **Server (Gaming/File Server):** Adding a server to the design goes beyond the minimal requirements (the assignment didn't explicitly list a server in the must-haves in the document, but the scenario calls for it). We justified including a server because a dedicated machine for game hosting ensures that game performance is not impacted

by someone's desktop being in use. The server can run 24/7, enabling persistent game worlds (Minecraft realm always online, etc.) and allow remote access to files. We picked a Dell PowerEdge tower server for its reliability (Xeon CPU with ECC RAM means it can run long periods without errors, and Dell servers have good support/warranties). While one might argue a custom-built PC could act as a server, the PowerEdge with Windows Server OS is chosen to demonstrate a professional approach: it will have features like RAID for data protection and remote management, which align with a high-quality setup. This is justified by the need for data safety (hence RAID1 and backups) given valuable game data or personal files might reside here. The cost is higher, but the server's role is crucial. It also offloads tasks from other PCs (for example, anyone can use their PC freely while the server does the heavy lifting for hosting games or storing backups). By using Windows Server, we ensure integration with Windows clients is smooth (sharing files, etc.), plus it can run most game server software which often targets Windows or Linux – we could have chosen Linux for the server OS to save cost, but Windows Server is chosen to leverage familiarity and certain game server ease (some game servers are easier to manage on Windows for a Windows-centric user).

In all, each desktop machine was chosen to exactly fit its intended purpose ("right tool for the job"). This avoids overspending on a task that doesn't need it (Office PC is modest) and underspending where performance matters (the CAD PC is beefy). We also ensured representation of all major OS platforms (Windows, macOS, Linux) as might be expected in a tech-savvy gaming household. This diversity showcases the network's ability to handle different systems.

6.3 Laptop and Mobile Device Choices

For portable devices:

- **Windows Office Laptop:** The Lenovo ThinkPad E14 was selected as a reliable, no-frills business laptop. The justification is that it offers durability (ThinkPads are known for solid build), a good keyboard (important for office work), and it's relatively light for portability. Its performance (Core i5, SSD) is enough for Office and web tasks, and its price is reasonable. We considered perhaps a cheaper consumer laptop, but those often compromise on build quality and may not last as long. The ThinkPad line also often includes features like TPM and better Linux compatibility if needed. This laptop allows the user to work from anywhere in the house or outside (its Wi-Fi keeps it connected). It being wireless tests and validates the network's wireless capability as well.

- **Windows Gaming Laptop:** The ASUS ROG Strix gaming laptop is justified to meet the "high-end laptop for gaming" requirement. While the user already has a high-end desktop, a gaming laptop allows flexibility – gaming in different locations or even at friends' houses/ LAN parties (portability), and it can double as a backup if the main gaming PC is busy or for co-op play in the same room. We chose a model with a powerful GPU (RTX 3070) to ensure it truly can handle modern games at high settings. ASUS's ROG series has good cooling for a laptop and is tailored to gamers with high refresh rate screen and RGB keyboard, etc. This choice shows that we are not solely relying on desktops for gaming; even the wireless network must handle a high-performance gaming client (hence Wi-Fi 6 is important). It's an expensive laptop, but justified by the scenario of a "fantasy network" where having such a device makes sense for a gaming enthusiast. It also can be used for VR if needed or as a secondary CAD machine if required.

- **MacBook Laptop:** We included a MacBook Pro to cover the Macintosh laptop requirement and to allow macOS mobility. The MacBook Pro 14″ M2 is chosen

because it offers a great balance of power and portability. The justification is that if someone in the environment is a Mac user (say a family member or the user themselves at times), they can carry this laptop to do their tasks on the go (coffee shop, travel) and then seamlessly integrate back into the home network. The M2 chip also has excellent battery life, meaning on Wi-Fi it can run for many hours – a nice benefit for a portable. The MacBook complements the iMac: one can sync files via iCloud, etc. We opted for the Pro model for extra performance in case any heavier tasks are needed on the go (like Xcode development or video editing). Apple's build quality and ecosystem integration are the key reasons – e.g., the MacBook can also easily AirPlay to an Apple TV or share screen to the iMac, etc., which might be part of the user's lifestyle.

- **Tablet (iPad):** The tablet is justified as a consumption device and auxiliary tool. An iPad Air with an M1 chip is almost as powerful as a laptop for many tasks, and can be used as a secondary screen (Sidecar feature with Macs) or to play mobile games, or control smart devices in the room (like lights, etc.). We included it to meet the requirement of a wireless tablet and chose a quality one (Apple) because it has a long software support cycle and a rich app ecosystem. It's useful to quickly check network status apps or as a console for streaming (e.g., stream gameplay from the server or main PC via Steam Link app to the iPad). While an Android tablet could have been chosen, the iPad was selected due to its popularity and the scenario already having Apple devices. It adds versatility to how the network might be used (e.g., using the tablet to RDP into the server or to take notes while gaming, etc.).
- **Smartphone:** The smartphone is included as most households would have one, and it's another device on the Wi-Fi. The Samsung Galaxy S22 represents a high-end Android phone which ensures Wi-Fi 6 connectivity and can act as a test device for

network health (since one can run speed tests on it or use it to receive network alerts from the router app). The justification is straightforward: a smartphone is a necessity and having it on the network is important for things like receiving any two-factor authentication codes for accounts, using it as a remote for the server (apps like TeamViewer or MS Remote Desktop client on phone), etc. We chose an Android to complement the iOS tablet – showing cross-platform support again. The Galaxy S22 has excellent Wi-Fi performance and modern features (and it's likely a device the user might already own or plan to get in a "dream setup").

- **Why Both Mac and Windows Laptops:** One might question if having both a Windows and Mac laptop is redundant. In this scenario, we assume possibly multiple people or multiple roles – e.g., the Windows gaming laptop is personal for gaming, the MacBook might be used by another household member or for work-related tasks if the user has a job that prefers Mac (or simply for familiarity with both OSes). Also, it demonstrates the network can handle different systems concurrently on Wi-Fi.

All mobile and laptop devices chosen are high-quality, name-brand (Lenovo, ASUS, Apple, Samsung) which tend to have good driver support and compatibility. This reduces the chance of weird network issues that can sometimes occur with very cheap devices using older Wi-Fi chips, etc. By investing in decent models, we ensure each device will perform well on the network and have a longer usable life.

6.4 Peripheral and Server Choices

Printer: The HP Color LaserJet M479fdw was chosen to provide a robust printing solution. The justification for a color laser over a cheaper inkjet is multi-fold: lasers have faster print speeds (useful if printing multi-page documents), the toner doesn't dry out (lower maintenance for a home that might go days without printing), and this particular model also offers scanning/copying which can be handy in a home office. Moreover, since one of the PCs

is used for photo editing, having a color printer allows occasional printing of photos or proofs (though a specialized photo inkjet would do better for gallery-quality prints, the laser is more all-purpose). This model has Ethernet and Wi-Fi, giving flexibility in placement. HP was chosen for its reliable driver support across all OS (Windows, macOS, Linux – all can print to it). This device supports AirPrint and Cloud Print features which align with modern use (printing directly from iPad or phone easily). The presence of a printer at all is often overlooked in purely gaming setups, but since this is also a home office, it's justified that one can print documents (like game guides, school/work documents, or even QR codes etc.). It adds to the completeness of the SOHO environment.

UPS: Including a UPS is an example of going above the basic requirements to "better the environment". The justification is that power outages or surges could interrupt gaming sessions or worse, corrupt data on the server during a sudden loss of power. By using an APC UPS for the critical devices (router, switch, server, and maybe the main PC), we protect the hardware and data. Even though not explicitly required, this shows a professional touch in the design, aligning with best practices for any office environment, even at home. The UPS chosen (1000VA) can keep the essentials running for a short time – enough to safely shut down the server if needed or ride out very brief outages. It also provides surge protection. Given the relatively high investment in equipment, a UPS is a modest addition to safeguard that investment. This choice is justified by the desire for network reliability – e.g., if the power flickers, the Wi-Fi and server will stay up, meaning an ongoing game server session isn't dropped and no one's work is lost unsaved.

Backup Drives/Strategy: While not a physical "device" choice like others, our inclusion of external backup drives and a cloud backup plan is important to justify. We plan to use a 4TB external HDD for server backups and perhaps smaller USB sticks or cloud for PC backups. The justification is straightforward: losing game data or important files can be devastating,

and since cost isn't a huge issue, spending a bit on backup storage is wise. This aligns with the 3-2-1 backup rule (multiple copies, different media, one off-site) which is considered a gold standard for data protection. By having a backup strategy, the network design doesn't just focus on uptime but also on data integrity and disaster recovery, which is often overlooked in home setups. This again shows going beyond minimum, a point the assignment notes students often forget (we made sure not to forget it).

Software Choices: Briefly justifying software – using Windows 11 Pro on capable machines is for features and future-proofing (Pro offers BitLocker, Remote Desktop, etc., which align with security and manageability). Using Windows Server on the server is justified for ease of integration as explained. Office 365 was chosen as it's the standard productivity suite needed for those Office tasks on the low-end machines; a free alternative (LibreOffice) could have been used to cut cost, but Office 365 ensures maximum compatibility if this network is used for any work-from-home scenario. For CAD and Adobe, we allocated licenses because using the latest software ensures the high-end hardware is fully utilized (and presumably the user in this fantasy can afford the subscriptions). We also mentioned anti-virus beyond Windows Defender to show consideration of layered security (some prefer a third-party suite for additional features like VPN or identity protection). In reality, Windows' built-in protections are quite good, but the inclusion is justified as part of a comprehensive security stance.

In conclusion, each component—be it a PC, a laptop, or a peripheral—was chosen with a mind to reliability, performance for its intended task, and integration into the whole. Nothing is "random": for example, the network printer with both Ethernet/Wi-Fi fits into any layout we choose; the UPS covers the key devices that matter for continuity; the server choice ensures hosting needs are met without compromise. By justifying in this manner, we demonstrate that the design is cohesive and every part serves a purpose aligned with the user's needs and project goals.

Security and Backup Considerations

Security is woven throughout the design, but here we summarize the key security configurations and backup plans to highlight our holistic approach to protecting the network and data (an area often forgotten, but explicitly required). Below are the measures in place:

- **Firewall & ACLs:** The router's firewall is configured with a default deny policy for inbound traffic. Only specific ports for the game server are opened. This greatly reduces attack surface. Additionally, the router's admin interface is not reachable from WAN, and UPnP is off to prevent rogue port mappings. Internally, all devices have their OS firewalls on as well (Windows Firewall on PCs, etc.), creating layered security (defense in depth). For example, even if a device got malware, its local firewall might prevent it from spreading or communicating out. We also could implement an ACL on the router to block known malicious domains or enable the router's AIProtection (Asus feature) which can automatically block malware communications – this is turned on for an extra layer.

- **Wi-Fi Security:** We use WPA3-Personal encryption, which is currently the strongest standard for home Wi-Fi, providing robust protection against cracking attempts. A strong passphrase (random, not easily guessable) is set. We avoid deprecated protocols (no WEP, no WPA-TKIP) as recommended. The SSID is not hidden (hiding SSID is not a real security measure and can cause connectivity issues). Instead we rely on the strong authentication of WPA3. If any device doesn't support WPA3, the transitional mode allows WPA2 with AES, which is still very secure. We also considered using a guest SSID to segregate untrusted devices – and indeed, if visitors need Wi-Fi, we have that option ready (with client isolation so guests can't snoop LAN resources).

- **Device Hardening:** Default passwords on all devices are changed (router admin, any default passwords on server or switches etc. – though switch is unmanaged, so no interface). The server and PCs enforce strong Windows account passwords. The Linux PC uses key-based SSH authentication if SSH is enabled, and firewall. Macs have their firewall on and both Macs and Windows have disk encryption (FileVault, BitLocker on laptops) to protect data at rest, especially for the portable devices. Auto-run of USB drives is disabled to prevent malware injection. Firmware on devices (router, etc.) will be kept updated – a practice which patches security vulnerabilities regularly.

- **Antivirus and Patching:** All computers run updated anti-malware tools (Windows Defender on Windows, possibly an additional AV as noted; ClamAV or equivalent on Linux if needed; Macs rely on XProtect built-in and maybe Malwarebytes if extra care). We enable periodic full scans. More importantly, all operating systems are set to update automatically to get security patches. Third-party apps (Adobe, etc.) are also updated. The server, being always on, is monitored closely for updates and has Windows Defender with real-time protection as well. Email scanning (though not detailed) would be handled on clients by their AV or by using webmail with providers that scan attachments.

- **Network Monitoring:** The router has logging enabled for firewall events – we can review if any port scans or blocked attempts occur. It can also send an alert if someone new joins the Wi-Fi (some routers have this feature), which can tip off if an unauthorized device connected. We decided not to implement a full IDS/IPS due to complexity, but note the Asus router does offer a basic IPS (Trend Micro's AIProtection). We turned that on as it can detect common patterns of attacks or infected devices calling out. This provides some intrusion detection on the edge. The

network is small, so manual monitoring (like checking router logs or using a tool like Pi-hole for DNS monitoring or Spiceworks for device inventory) is feasible occasionally.

- **Physical Security:** The equipment (router, switch, server) is ideally placed in a corner of the room or a ventilated closet where accidental tampering is minimized. The server chassis has a lockable side panel (common in Dell servers) to prevent someone pulling drives out. The networking gear is behind the desk, etc. While this is a home setting, we consider that an intruder who gains physical access could compromise things, so doors to the room are kept locked when not in use, etc. The UPS also mitigates one physical risk – power loss – which can be a vector for data corruption.
- **Backup Strategy:** We implement a rigorous backup scheme for critical data. The game server world data and configuration is backed up daily to both an external HDD (connected to the server) and a cloud service (perhaps using OneDrive or a specialized cloud backup like Backblaze). This ensures that even if the server hardware fails or data is ransomware-encrypted, we have offline backups to restore from. User PCs are encouraged to store important docs on the server or a synced cloud folder which gets backed up. The Windows PCs have “File History” enabled to the server’s shared drive (so they keep versioned backups of user libraries on the server, which itself is backed up). The Mac users can use Time Machine to the server (Windows Server can serve as an SMB Time Machine target with some configuration). At minimum, the MacBook will use an external drive for Time Machine periodically. The Linux PC might use rsync to copy important files to the server or a cloud. We thus attempt the 3-2-1 rule: at least 3 copies (live data, local backup, offsite backup) on 2 different media, 1 offsite. Offsite could be cloud or even an external drive periodically taken to another location like Dr. Wallace does once a week to the bank or once a month to his office at

school. This way, even catastrophic events (fire, theft) would not result in total loss and maximum loss of data is a week (if the copy stored at the bank is ok) or a month if the backup at the school is ok.

- **Recovery Planning:** We maintain a document (could be part of this design deliverable or kept separately) that lists all device credentials, IPs, and recovery steps. For instance, instructions on how to restore the server from backup, or how to re-configure the router if it resets. We also backup the router configuration file after setting it up, so it can be reloaded if the router is replaced or factory reset – saving time and ensuring all those port forwards and DHCP reservations are not lost. The presence of multiple devices means if one fails, others might serve as temporary stand-ins (e.g., if the high-end desktop fails and something urgent needs to be done, the gaming laptop or Linux PC can step in). The network has some redundancy in capability if not in hardware (except the single router – which is a single point of failure; one might consider keeping the old ISP router as a backup just in case).

- **User Awareness:** Since this is a home setup, user education is relevant: the users will follow safe practices like not downloading unknown attachments, using unique strong passwords for different accounts (managed with a password manager perhaps), and enabling two-factor authentication on important accounts (game accounts, cloud storage, etc.). The smartphone can be used for 2FA, adding security to online services related to gaming or work. We also ensure the Wi-Fi passphrase is shared only with authorized people and changed if there's any suspicion of it being known publicly.

By addressing security in multiple layers (network edge, device config, user behavior) and by implementing a solid backup routine, this design mitigates major risks that a home network could face: hacking, malware, data loss, and downtime. The combination of a strong firewall and modern Wi-Fi encryption defends against outside intrusion, while up-to-date devices and

AV defend against threats that might come through user actions. Backups and UPS guard against data and power disasters. Thus, the network is not only fast and functional, but also safe and resilient against both cyber and physical threats, which is crucial for any environment where valuable data and services are present.

Conclusion

In conclusion, the proposed SOHO network design for the gaming room meets all specified requirements and provides a high-performance, secure, and reliable environment for both work and play. We have included every required device type – multiple PCs (Windows, Linux, Mac), laptops, mobile devices, printer, switches, and a dedicated server – and detailed their specifications and configurations. The network is built with quality components prioritizing performance (Gigabit+ speeds, Wi-Fi 6) and security (firewalls, WPA3, backups).

This design not only fulfills the project's checklist but also goes beyond by incorporating best practices such as using a UPS for power protection and a comprehensive backup strategy to safeguard data. The electronic diagram and legend clearly illustrate the network topology, and the configuration section spells out how each piece will be set up (from IP addresses to firewall rules) to function harmoniously. The Bill of Materials demonstrates that all elements have been accounted for, and the justifications show the thoughtful reasoning behind each choice.

Ultimately, this "fantasy network" is scalable and future-proof: there is room for expanding wired devices via the switch, the Cat6 cabling supports future higher speeds, the router can handle faster internet or more devices if needed, and the server and workstations have enough headroom for new software demands. The user(s) of this network can confidently engage in online gaming, content creation, and daily computing tasks knowing that the network will deliver low latency, high throughput, and strong security.