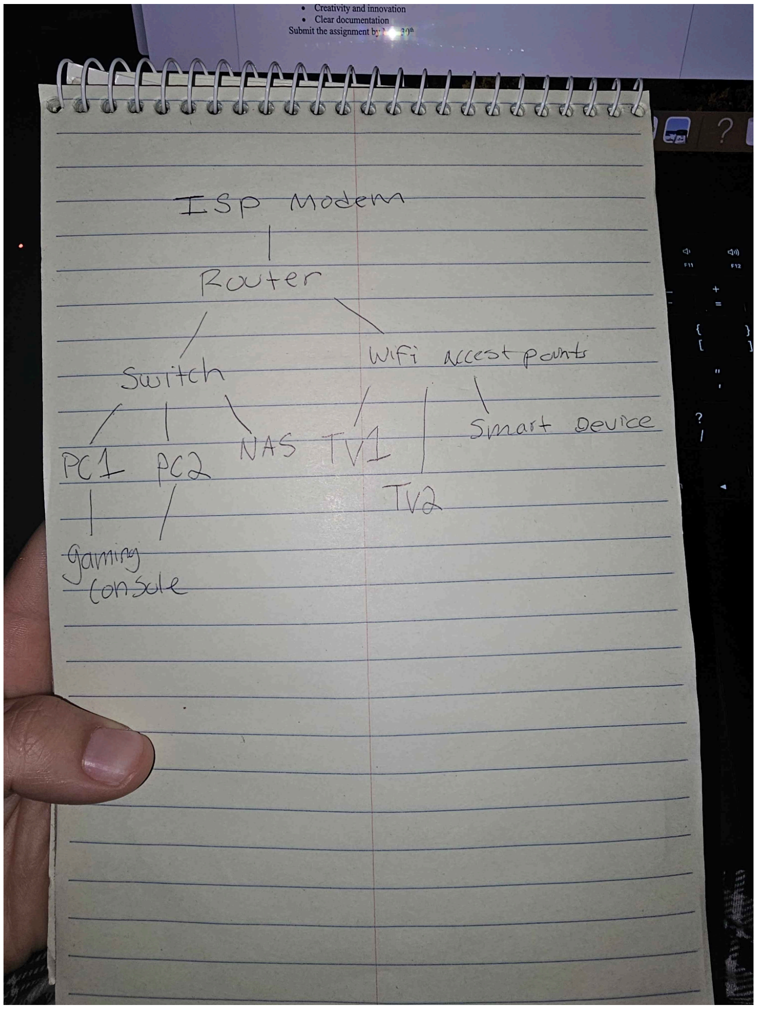
Network Topology: Hybrid Star Topology



Network Devices:

Router

- Model: ASUS RT-AX88U
- Features: Integrated firewall, VPN support, VLAN capability, robust security features, and high-speed Wi-Fi.
- Configuration:
    - Network Address: 192.168.1.1
    - Subnet Mask: 255.255.255.0
    - DHCP Range: 192.168.1.100 to 192.168.1.200
    - Security: Enable firewall, configure VPN for remote access, set up VLANs for segmentation (e.g., VLAN 10 for remote workers, VLAN 20 for family devices, VLAN 30 for IoT devices).

    - Wi-Fi Configuration: Set SSIDs, enable WPA3 encryption, create a separate guest network.

Switch

- Model: Netgear GS108Ev3
- Configuration:
    - IP Address: Assign a static IP within the router’s range.
    - VLAN Setup: Configure VLANs to segregate traffic (VLAN 10 for remote worker devices, VLAN 20 for home devices, VLAN 30 for smart home devices).

Wireless Access Points (APs)

- Model: TP-Link EAP245
- Configuration:
    - IP Address: Assign static IPs to each AP within the router’s range (192.168.1.3 for AP1, 192.168.1.4 for AP2).
    - SSID Configuration: Ensure SSIDs match those set on the router for seamless roaming.
    - Security: Enable WPA3 encryption, configure guest network, and ensure APs are on the correct VLANs.

NAS Device

- Model: QNAP TS-251D
- Configuration:
    - IP Address: Assign a static IP (192.168.1.10).
    - Access Control: Set up user accounts and permissions, enable secure access protocols (e.g., HTTPS, SFTP).
    - Backup Configuration: Configure automated backups for critical data.

Device Breakdown

1. Remote Workers (VLAN 10)
    - Devices: 2 Laptops/Desktops
    - Connection: Primarily Ethernet for stability and speed; Wi-Fi as a secondary option
2. Teenagers (VLAN 20)
    - Devices: 2 Laptops/Tablets/Smartphones
    - Connection: Primarily Wi-Fi for mobility; Ethernet available if needed
3. Gaming Console (VLAN 20)
    - Device: Xbox or PlayStation
    - Connection: Ethernet for low latency and high performance in gaming
4. Smart TVs (VLAN 20)
    - Devices: 2 Smart TVs
    - Connection: Ethernet for reliable and uninterrupted streaming; Wi-Fi as a backup
5. NAS Device (VLAN 20)
    - Device: QNAP TS-251D

    - Connection: Ethernet for high-speed access to stored media and backups.

6. Smart Home Devices (VLAN 30)
    - Devices: Various smart home devices such as smart lights, thermostats, cameras, etc
    - Connection: Wi-Fi, typically requires low bandwidth.

IP Addressing Scheme and Subnet Structure

Network Address: 192.168.1.0/24
Subnet Mask: 255.255.255.0
Gateway (Router) IP: 192.168.1.1

IP Address Ranges:

- Router and Core Network Devices: 192.168.1.1 - 192.168.1.4
- Static IPs for Key Devices:
    - NAS Device: 192.168.1.10
    - Gaming Console: 192.168.1.20
    - Smart TVs: 192.168.1.30, 192.168.1.31
    - Remote Worker Desktops: 192.168.1.40, 192.168.1.41
- DHCP Range: 192.168.1.100 - 192.168.1.200
- Smart Home Devices (IoT): 192.168.1.50 - 192.168.1.70

Security Measures

Firewall Configuration

- Router Firewall:
    - Enable Stateful Packet Inspection (SPI): Ensure the router's firewall has SPI enabled to inspect incoming packets for irregularities.
    - Set Up Firewall Rules: Allow necessary traffic (e.g., HTTP, HTTPS, DNS) for normal operations. Deny all other inbound traffic by default to prevent unauthorized access.
    - Port Forwarding: Only set up port forwarding rules for essential services.
    - Logging: Enable logging for firewall activities to monitor and review any suspicious activities.

Virtual Private Network (VPN) Configuration

- VPN Type: ProtonVPN for secure and efficient VPN connections.
- Configuration Steps:
    - Install VPN Server on router

    - User Authentication: Use strong authentication methods (certificates, multi-factor authentication) to secure VPN access.
    - Client Configuration: Distribute VPN client configuration files to remote users for secure access.

Wireless Security

- Encryption: Enable WPA3 encryption on all Wi-Fi networks for enhanced security. If devices do not support WPA3, use WPA2 as a fallback.
- SSID Naming: Use unique SSIDs that do not reveal personal information or the network's purpose.
- Guest Network: Create a separate guest network for visitors. Isolate guest traffic from the main network using VLANs.
- MAC Address Filtering: Enable MAC address filtering to allow only known devices to connect to the network. This can add an additional layer of security but should not be relied upon solely.

VLAN Configuration

- VLAN 10: Remote Workers
    - Devices: Laptops, desktops
    - Security: Ensure VLAN 10 is isolated from other VLANs except where necessary.
- VLAN 20: Family Devices
    - Devices: Teenagers' devices, smart TVs, gaming console
    - Security: Restrict access to sensitive devices (NAS) from VLAN 20.
- VLAN 30: IoT Devices
    - Devices: Smart home devices
    - Security: Isolate VLAN 30 from other VLANs to prevent potential breaches from less secure IoT devices.

Device Security

- NAS Device Security:
    - Firmware Updates: Regularly update the NAS firmware to protect against vulnerabilities.
    - Access Control: Set up user accounts with strong passwords and appropriate permissions.
    - Secure Access Protocols: Enable HTTPS, SFTP, and other secure protocols for accessing NAS.
    - Firewall: Enable the NAS's built-in firewall to restrict access to specific IP addresses or subnets.
- End-Device Security:
    - Operating System Updates: Regularly update operating systems and software to patch security vulnerabilities.
    - Strong Passwords: Use strong, unique passwords for all devices, don't use the same password for every device
    - Multi-Factor Authentication (MFA): Enable MFA where possible, especially for remote access and critical accounts.

Remote Access

Configure VPN on Router

- Set up ProtonVPN on the router.
- Generate and distribute VPN client configuration files to remote workers.
- Ensure firewall rules allow VPN traffic.

Secure NAS Access

- Enable secure protocols (HTTPS, SFTP).
- Create user accounts and assign permissions.
- Make NAS accessible via VPN.

Implement Additional Security Measures

- Enable 2FA.
- Use strong passwords.
- Keep firmware updated.
- Implement ACLs.

Monitoring and Management

- PingPlotter: For troubleshooting connectivity issues.
- Regular updates and patches for all devices.
- Strong access control and MFA for management interfaces.
- Regular configuration backups.

Security Measures

- Enable firewall and VPN on the router.
- Use WPA3 encryption for Wi-Fi and create a guest network.
- Review logs regularly for unauthorized access.
