The new office in Fayetteville, NC, needs a strong and flexible network that supports company operations. It must allow employees to work remotely while ensuring smooth communication and data sharing. The OSI model, which explains how devices connect and communicate, was used to design this network. Each layer of the OSI model was carefully considered to make sure the network runs efficiently. The physical layer will use high-quality Ethernet cables and fiber-optic connections for reliability. The network layer will handle IP routing with a private IP address range to prevent conflicts and maintain smooth operations. This setup will also support company growth by enabling secure remote work and data protection.

A star topology is the best choice for the local network because it connects all devices to a central switch. This makes it easy to expand, improves network speed, and helps quickly identify issues when troubleshooting. The central switch will be a high-performance managed switch with VLAN support to organize network traffic efficiently. Backup switches will be available to keep the network running in case of equipment failure.

For internet service, fiber-optic internet is recommended because it provides fast speeds, a stable connection, and low delays, which are important for video calls and remote work. A dedicated leased line with a Service Level Agreement (SLA) will guarantee reliable service. A second internet provider will also be set up as a backup in case the primary connection goes down.

The office will need high-quality network equipment, including enterprise-grade switches, routers, and firewalls. A next-generation firewall will be installed to provide security features such as deep packet inspection, intrusion prevention, and VPN access for remote employees. Wi-Fi 6 access points will be used to provide strong wireless coverage, ensuring all employees stay connected. The network will also separate guest Wi-Fi from business traffic to improve security. Employee computers will be protected with antivirus software, VPN access, and data security tools. Endpoint detection and response (EDR) solutions will be used to monitor for cyber threats in real-time and prevent attacks.

To handle printing, a cloud-based system will send print jobs securely to the Albany headquarters. Printer drivers will be managed centrally to ensure compatibility, and access controls will limit printing to authorized users. A secure print release system will require employees to confirm their identity before retrieving documents, reducing the risk of sensitive information being accessed by the wrong person. A tracking system will monitor and optimize printing efficiency to prevent waste.

To support video meetings, a 500 Mbps fiber connection will be set up. The network will prioritize video call traffic using Quality of Service (QoS) settings to prevent lag or disruptions. A dedicated conference room will include high-definition cameras, noise-canceling microphones, and large display screens to enhance virtual meetings. Redundant power supplies and an uninterruptible power supply (UPS) will be installed to keep equipment running during power outages.

Common network problems like slow speeds and connectivity issues will be managed with network monitoring and traffic prioritization. Troubleshooting tools like ping tests, traceroute, and network analyzers will be used to quickly identify and resolve issues. Backup switches and routers will be kept on-site for fast replacements in case of hardware failure. Automated network monitoring tools like Nagios or SolarWinds will track network performance, detect issues, and send alerts to IT staff when problems arise.

To ensure the network stays secure and runs smoothly, monitoring tools will continuously check performance and minimize downtime. Software updates and security patches will be applied automatically to keep systems protected. A structured patch management system will schedule and deploy updates efficiently. A tracking system will be used to monitor all network devices and software licenses, ensuring compliance and preventing unauthorized access. Regular security audits will be conducted to evaluate the network’s safety and efficiency.

This network design provides a secure, scalable, and efficient setup for the new Fayetteville office. By following best practices and incorporating backup options, security measures, and expansion capabilities, the company will be able to support employees and continue growing successfully.

Cisco. (n.d.). *What is a firewall?* Cisco. Retrieved from https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

IEEE. (2023). *Wi-Fi 6: The next generation of wireless technology.* Institute of Electrical and Electronics Engineers. Retrieved from<https://www.ieee.org/wifi6>

Nagios. (n.d.). *Network monitoring software.* Retrieved from<https://www.nagios.org>

SolarWinds. (n.d.). *Network performance monitoring.* Retrieved from https://www.solarwinds.com/network-performance-monitor

Microsoft. (2023). *Endpoint detection and response (EDR).* Retrieved from<https://www.microsoft.com/security/edr>

U.S. Cybersecurity & Infrastructure Security Agency (CISA). (2023). *Patch management best practices.* Retrieved from https://www.cisa.gov/patch-management