**Part 2: Hybrid Working Environment Design for College Faculty and Students**

**Task 1: Explore Options for Achieving Secure Hybrid Network Access**

**Hierarchical Network Design:**

* **Core Routers, Multilayer Switches, and Access Switches:**
  + Implement a hierarchical model to ensure efficient data flow and management. Core routers will connect to multilayer switches, which will then connect to access switches in each department.
  + **Redundancy Strategies:**
    - Include redundancy measures such as dual connections to critical devices and backup power supplies to enhance network reliability.

**VLANs and Subnetting:**

* **VLAN and Subnet Allocation:**
  + Allocate specific VLANs and subnets for each department, using the 192.168.100.0 base network to manage traffic securely and efficiently.
  + **VLAN Configurations:**
    - Apply VLAN configurations to switches to isolate and manage departmental traffic, enhancing security and performance.

**Security Measures:**

* **Access Control Lists (ACLs):**
  + Configure ACLs to restrict access to sensitive areas and services, ensuring that only authorized users can access specific resources.
* **Virtual Private Network (VPN):**
  + Implement VPN solutions to provide secure remote access for faculty and students. This ensures encrypted communication and access to campus services from off-site locations.
* **Port-Security:**
  + Enforce port-security measures to prevent unauthorized devices from connecting to the network, safeguarding against potential breaches.

**Routing Protocol (OSPF):**

* **Dynamic Routing with OSPF:**
  + Deploy OSPF to enable dynamic routing and efficient route advertisement, ensuring seamless connectivity across the network.

**DHCP Configuration:**

* **DHCP Servers:**
  + Establish DHCP servers in the server room for dynamic IP address allocation. Assign static IP addresses to critical devices to ensure stability.

**Monitoring and Testing:**

* **Network Monitoring Tools:**
  + Integrate advanced monitoring tools to track performance and security in real-time.
* **Comprehensive Testing:**
  + Conduct thorough testing of communication channels, DHCP services, OSPF routing, VPN connectivity, and security measures to ensure effectiveness.

**Task 2: Update the Campus Network Topology with New Components**

**Network Design and Topology Implementation:**

* **Detailed Network Topology:**
  + Developed a comprehensive topology outlining the placement of routers, switches, and servers.
  + **Core Routers and Switches:**
    - Configured core routers, multilayer switches, and access switches to optimize network performance and management.

**VLANs and Subnetting Configuration:**

* **VLAN Allocation:**
  + Planned and implemented VLAN allocations for each department to ensure scalability and efficiency.
  + **VLAN Implementation:**
    - Applied VLAN configurations on respective switches to manage and isolate traffic.

**Security Measures Implementation (ACLs, VPN, Port-Security):**

* **Access Control Lists:**
  + Defined stringent ACLs to control user access and protect sensitive resources.
* **VPN Solutions:**
  + Implemented VPNs for secure remote access, ensuring encrypted communication channels.
* **Port-Security:**
  + Set up port-security measures to prevent unauthorized access to network ports.

**Routing Protocol Configuration (OSPF):**

* **OSPF Deployment:**
  + Deployed OSPF across routers and switches to facilitate dynamic routing and route advertisement.

**DHCP Server Setup and Testing:**

* **DHCP Servers:**
  + Established and configure DHCP servers in the server room for dynamic IP address allocation.
  + **Testing:**
    - Conducted extensive testing to validate DHCP functionality and effectiveness.

**Network Monitoring Tool Implementation:**

* **Monitoring Tools:**
  + Deployed advanced monitoring tools for real-time performance and security tracking.
  + **Proactive Issue Resolution:**
    - Ensured proactive identification and resolution of potential network issues.

**Task 3: Explain the Reasoning Behind Choices and Detail Risks and Advantages**

**Reasoning Behind Choices:**

* **Hierarchical Network Design:**
  + A hierarchical model ensures efficient data management, scalability, and redundancy, enhancing overall network performance and reliability.
* **VLANs and Subnetting:**
  + VLANs and subnets provide secure traffic segmentation and efficient network management, reducing the risk of unauthorized access and improving performance.
* **Security Measures:**
  + ACLs, VPNs, and port-security measures ensure robust protection against unauthorized access, data breaches, and other security threats.
* **Routing Protocol (OSPF):**
  + OSPF enables dynamic and efficient routing, ensuring seamless connectivity and optimal network performance.
* **DHCP Configuration:**
  + DHCP servers facilitate dynamic IP address allocation, ensuring efficient management and connectivity of devices.
* **Monitoring and Testing:**
  + Advanced monitoring tools and comprehensive testing ensure continuous performance tracking and security, allowing proactive issue resolution.

**Risks and Advantages:**

**Advantages:**

* **Enhanced Security:**
  + Robust security measures (ACLs, VPNs, port-security) protect against unauthorized access and data breaches, ensuring data confidentiality, integrity, and availability.
* **Operational Efficiency:**
  + Streamlined communication, dynamic IP allocation, and efficient routing (OSPF) improve overall network efficiency.
* **Cost-Efficiency:**
  + Internal management of the network infrastructure reduces reliance on third-party services, lowering operational costs.
* **Reliability:**
  + Redundancy strategies and a hierarchical design increase network reliability and ensure continuous availability.

**Risks:**

* **Complexity:**
  + Implementing a hierarchical network design with multiple security measures can be complex and may require advanced technical expertise.
* **Initial Cost:**
  + Initial setup costs for advanced hardware and monitoring tools can be high, although long-term savings and efficiency gains will offset this.
* **Maintenance:**
  + Ongoing maintenance and updates are required to ensure security and performance, demanding regular attention and resources.

By implementing this comprehensive methodology, the college will establish a secure and efficient hybrid working environment for faculty and students, ensuring seamless access to resources and services both on-campus and remotely.