## DOCUMENTATION:

### About St. Mary's University:

St. Mary's University - Around Mexico is a prominent institution known for its commitment to academic excellence and diverse learning opportunities across Mexico. Spearheading the network administration is Markos Tegestu, an adept professional dedicated to ensuring seamless connectivity and technological advancements within the university.

### It’s Network Infrastructure:

At St. Mary's University - Around Mexico, a sophisticated network infrastructure is meticulously designed to cater to the diverse needs of its campus environment. Wide Area Network (WAN) configurations are implemented to effectively connect and separate various buildings, ensuring efficient communication and data transfer across the campus premises. Additionally, Local Area Network (LAN) setups are strategically deployed to separate different floors within buildings, optimizing connectivity and resource sharing among specific departments or areas. To further enhance accessibility and flexibility, Wireless Local Area Network (WLAN) systems are integrated, specifically targeting floors requiring wireless connectivity, facilitating seamless access to resources and services across these designated areas. This comprehensive approach to network infrastructure at St. Mary's University ensures reliable and tailored connectivity solutions throughout the campus.

### The purpose of the Network:

The network at St. Mary's University - Around Mexico serves a dual purpose: facilitating seamless data sharing through a dedicated FTP server for local data exchange, while also ensuring efficient internet access across separate floors within the campus. This setup enables effective collaboration through local data sharing while providing each floor with reliable connectivity to the internet for various academic and administrative needs.

### Server Computers:

St. Mary's University employs three crucial servers within its network infrastructure: DHCP, DNS, and FTP servers. The DHCP server efficiently allocates IP addresses, ensuring seamless connectivity for devices across the campus. The DNS server manages domain names, translating them into IP addresses for smooth navigation and accessibility. Additionally, the FTP server stands as a dedicated platform for local data sharing among users within the university, fostering collaborative efforts. This setup supports the primary network goals of enabling reliable connectivity, streamlined data exchange through FTP, and efficient internet access across the various floors of the campus.

**Security:**
At St. Mary's University, a robust security framework is implemented to safeguard the network infrastructure and sensitive data. This includes comprehensive measures such as firewalls that act as barriers against unauthorized access and malicious threats. Antivirus software is deployed across the network to detect and prevent the intrusion of malware or viruses that could compromise system integrity. Additionally, intrusion detection systems are employed to actively monitor network traffic and swiftly identify any suspicious activities or potential breaches, allowing for immediate response and mitigation. These combined security measures create a multi-layered defense, ensuring the protection of the university's network and data against various cyber threats.

**Security Protocols & Update Time:**
At St. Mary's University, security protocols and devices undergo regular updates and reviews within a stringent **six-month** cycle. This proactive approach ensures that the network's security measures remain current, robust, and capable of addressing emerging threats and vulnerabilities effectively. Regular reviews and updates help maintain the resilience of the university's security infrastructure, providing ongoing protection against evolving cyber threats.

**VPN?**
At St. Mary's University, there isn't a Virtual Private Network (VPN) implemented for remote access at the moment.

**Type of internet connection:**
St. Mary's University utilizes a high-speed fiber optic cable connection, providing substantial bandwidth to support the diverse internet needs across its campus infrastructure.

**Network Administration:**
Markos Tegestu, as the Network Admin, shoulders the responsibility for network administration and maintenance at St. Mary's University. He oversees the upkeep, configuration, and overall management of the network infrastructure to ensure its smooth operation and reliability.

**Monitoring Tools:**
At St. Mary's University, they currently do not employ any specific network monitoring tools or software for their monitoring and maintenance purposes.

**Network Performance Review:**
At St. Mary's University, network performance undergoes a daily review and assessment, ensuring ongoing monitoring and prompt identification of any issues or irregularities. This routine check-up helps maintain optimal network functionality and swiftly addresses any emerging concerns.

**Wireless Technologies:**
St. Mary's University implements 802.11g (Wi-Fi 3) and 802.11n (Wi-Fi 4) wireless technologies to support their wireless network infrastructure.

To ensure robust wireless security, St. Mary's University utilizes the WPA2 encryption protocol. This encryption standard enhances the security of their wireless network by safeguarding data transmitted over Wi-Fi connections, providing a strong defense against unauthorized access and potential security breaches.

**Future Plans:**
St. Mary's University has strategic plans for network enhancement, including the replacement of failed switches to optimize network stability. They aim to implement patch panels for structured cabling, enhancing organization and efficiency. Upgrading older cables and computers is on the agenda to improve performance and reliability. Additionally, plans include upgrading the Uninterruptible Power Supply (UPS) systems to bolster power backup and ensure uninterrupted network operations. These initiatives align with the university's commitment to modernizing infrastructure and maintaining a robust network environment.

**Challenges:**
The university faces a challenge due to employees' limited awareness of the network infrastructure. Addressing this challenge might involve conducting educational sessions or workshops to enhance understanding and familiarity with the network's functionalities, benefits, and best practices. Increasing communication and providing resources could empower employees to utilize the network more effectively, potentially improving overall productivity and security within the institution.