

1. PROBLEM STATEMENT

Configuring network switches is essential for network segmentation, managing traffic flow, and decreasing security risks. The task is complex, time-consuming, requires specialized expertise, and is prone to human error. Our solution, NetCommand, addresses this challenge with an affordable, user-friendly web application that streamlines switch configuration through a guided interface and a mobile-accessible terminal.

1.1. Need Statement

According to the 2023 Uptime Institute Data Center Resiliency Survey, misconfigurations and change management failures account for 45% of major network-related outages [1]. With 33.1 million small businesses in the U.S. relying on stable networks for operations like telephony, video conferencing, and multimedia, minimizing errors is critical. However, IT budgets are tight—only 9% is allocated to security, and 60% of organizations plan further cuts [2]. To address this issue, an efficient, accessible solution is needed to simplify switch configuration, reduce human error, and help IT teams manage growing network demands without requiring extensive expertise or additional resources.

1.2. Objective Statement

This project aims to develop a web application that simplifies network switch configuration through an intuitive interface, eliminating the need for IT professionals to carry laptops in data centers. The application will minimize errors, streamline configurations, and enhance accessibility by enabling secure, remote switch management via a mobile-friendly terminal.

1.3. Background and Related Work

NetCommand revolutionizes switch management by providing mobile terminal access and an easy-to-use interface. Traditionally, network administrators rely on SSH clients resembling PuTTY, requiring them to manually input complex commands while carrying bulky laptops. According to ECU Online Programs, network administrators are responsible for maintaining reliable systems, often under high workloads [3]. Enterprise solutions such as Cisco DNA Center and SolarWinds offer powerful features but come with high costs and require specialized expertise. While IT generalists receive training on such tools, they often lack advanced networking skills [4]. NetCommand offers a simpler, more cost-effective alternative, allowing users to execute pre-configured actions or input commands directly. Designed for IT administrators, network engineers, and field technicians, it provides quick access, vendor compatibility, and a robust tech stack with SSH encryption, MFA, and mobile frameworks for secure and efficient network management.

2. DESIGN REQUIREMENT SPECIFICATIONS

This section delineates the marketing requirements, engineering design specifications, constraints, and standards considered during the development phases of NetCommand—prototyping, testing, and implementation. NetCommand is crafted to fulfill functional and performance-based criteria, ensuring it effectively meets user needs and streamlines network management.

2.1. Requirements

NetCommand is designed to cater to the needs of a diverse user base, from IT novices to seasoned professionals, by providing a robust yet intuitive solution for network switch configuration. The requirements are split into customer-facing marketing requirements and technical engineering design requirements, each tailored to enhance usability and performance.

2.1.1. Marketing Requirements

NetCommand must fulfill the following core customer needs:

1. Web-based User Interface – The system provides an intuitive web-based UI for configuring switches, allowing easy VLAN creation and port assignments.
2. Secure Configuration Execution – Network changes are applied reliably and securely to prevent misconfigurations or unauthorized access.
3. Automation Options – NetCommand will utilize automation to make using its features easier and more intuitive.
4. Local and Direct Connectivity – The system functions without requiring internet access, allowing direct USB-C to Raspberry Pi connections for offline environments.

Figure 2-1 shows the objective tree that lays out the device's goals.

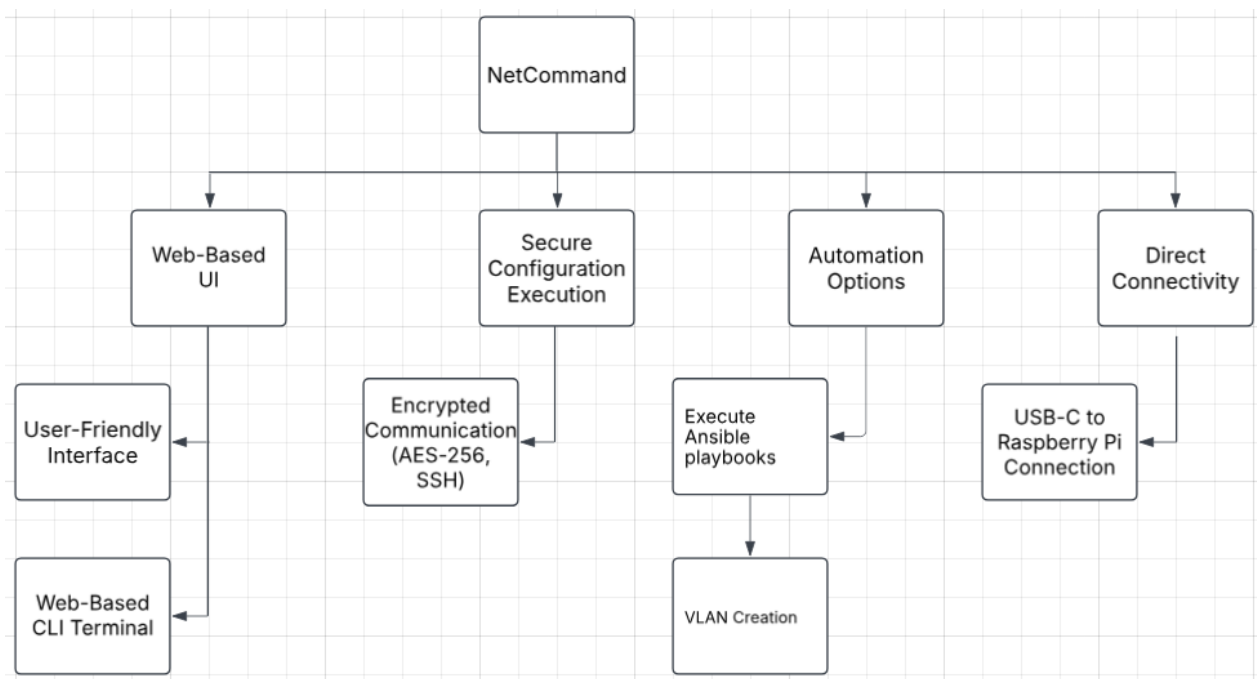


Figure 2-1: Objective Tree for NetCommand

The objective tree outlines NetCommand's primary goals and objectives, categorized based on key engineering and marketing requirements.

2.1.2. Engineering Requirements

Table 2-1 presents the engineering requirements that must be met to satisfy the marketing requirements enumerated in Section 2.1.1.

Table 2-1: Engineering Design Requirements

Number	Engineering Requirements	Description
1	NetCommand features a web-based user interface (UI).	This interface allows users of all technical levels to configure switches easily, enhancing the user experience by reducing complexity.
2	NetCommand includes a web-based command-line interface (CLI).	Displays live terminal feed for monitoring switch output and feedback
3	All network changes are executed through secure channels with AES-256 encryption.	These security measures ensure that configurations are applied reliably, protecting against unauthorized access and maintaining network integrity.
4	Execute Ansible playbooks.	Enables automated deployment and configuration management for network setups.
5	NetCommand allows direct connections via USB-C to Raspberry Pi interfaces.	Allows wired connection between device and network device.
6	NetCommand demonstrates automated VLAN Creation	NetCommand will be able to configure VLANs and assign ports to VLANs

Marketing Requirements

Number	Marketing Requirements	Description
1	Web-based User Interface	NetCommand provides an intuitive web-based UI for configuring switches, allowing easy VLAN creation and port assignments.
2	Secure Configuration Execution	Network changes are applied reliably and securely to prevent misconfigurations or unauthorized access.
3	Automation Options	NetCommand will utilize automation to make using its features easier and more intuitive.
4	Local and Direct Connectivity	NetCommand functions without requiring internet access, allowing direct USB-C to Raspberry Pi connections for offline environments.

NetCommand is designed to streamline network switch configuration through an intuitive web-based user interface (UI) that simplifies VLAN creation and port assignments. By reducing complexity, this interface enables users of all technical skill levels to efficiently configure network settings. For more advanced

interactions, NetCommand includes a web-based command-line interface (CLI) supporting both SSH and Serial protocols, allowing real-time execution of switch commands. A live terminal feed displays switch output, providing immediate feedback and monitoring capabilities.

Security is a core component of NetCommand, ensuring all network changes are executed through AES-256 encrypted channels, with multi-factor authentication (MFA) options available for controlled access. These security measures prevent unauthorized modifications, maintaining the integrity and reliability of network configurations. Additionally, the system integrates Ansible automation, enabling users to execute playbooks for VLAN creation, access port assignments, and trunk configurations. This functionality ensures automated, consistent, and efficient deployment of network settings across multiple devices.

To support flexibility and secure local access, NetCommand allows direct USB-C connections to Raspberry Pi interfaces, eliminating the need for external networking dependencies. This capability ensures the system remains functional in isolated or high-security environments, providing reliable switch management without requiring internet access.

2.2. Constraints

Table 2-2 describes several constraints imposed on the design process of NetCommand.

Table 2-2: Constraints

Type	Name	Description
Economic	Budget	The funds allocated to this project may not exceed \$1000.
Economic	Time	The development of the NetCommand system follows a two-semester timeline.
Manufacturability	Size	The physical dimensions of the NetCommand rack plug-in must be thinner than 2.5” and not exceed a length of 19”.
Health and Safety	Safety	To avoid injury to the user, NetCommand is built with a hard shell module around the Raspberry Pi and other connection points.
Health and Safety	Security	Utilizing encryption and security standard will limit the amount risk for possible infiltration and unauthorized access.

The total budget allocated for the NetCommand system is \$1,000, as specified under the “Budget” constraint. This funding must cover all necessary hardware, software, and prototyping costs, ensuring a cost-effective development process. The project is also subject to the “Time” constraint, which requires that all development and testing be completed within a two-semester timeline to meet academic deadlines.

To ensure compatibility with standard networking infrastructure, the “Size” constraint mandates that the rack-mounted module must be thinner than 2.5 inches and no longer than 19 inches. This ensures that NetCommand can be seamlessly integrated into existing network racks without exceeding space limitations.

The “Safety” constraint addresses potential risks associated with exposed electrical components. To prevent injury, a durable hardshell casing encloses the Raspberry Pi and all connection points, reducing the risk of accidental contact with electrical circuits.

Enclosing electronic components introduces potential overheating concerns, making ventilation essential for maintaining system stability. The “Ventilation” constraint specifies that vents and fans are incorporated into the housing to regulate internal temperature and prevent heat-related damage to sensitive components.

2.3. Standards

Table 2-3 lists all standards to which NetCommand adheres; these are technology standards as well as industry standards.

Table 2-3: Standards

Specific Standard	Standard Document	Specification / Application
IEEE Std 802.3-2018	IEEE Standard: <i>IEEE Standard for Ethernet</i> [6]	The application uses Ethernet connectivity to communicate with network switches, supporting various speeds (10Mbps to 10Gbps) for reliable device configuration.
IEEE Std 802.1Q-2018	IEEE Standard: <i>IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks</i> [7]	The backend implements VLAN tagging functionality, allowing users to configure virtual networks through the tablet interface without manual CLI commands.
IEEE Std 802.1D-2004	IEEE Standard: <i>IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Bridges</i> [8]	The system supports Spanning Tree Protocol configuration to prevent network loops when setting up switch interconnections.
IEEE Std 802.1X-2020	IEEE Standard: <i>IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control</i> [9]	The application enables configuration of port-based security features, protecting network access points from unauthorized connections.
Cisco Discovery Protocol (CDP)	Cisco Systems, Inc., Proprietary Protocol (Ethernet type: 0x2000) [5]	The backend utilizes CDP to automatically discover and identify Cisco switches on the network, gathering device information to streamline configuration.
IEEE Std 802.11-2020	IEEE Standard: <i>IEEE Standard for Information Technology—Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications</i> [10]	The tablet interface can utilize wireless connectivity and support configuration of wireless network settings on compatible switches.

Telnet RFC 854	Telnet protocol specification [11]	Telnet is a text-based network protocol that allows remote access to devices over TCP port 23. It enables bidirectional communication between a client and a server. However, it does not encrypt data, making it insecure for modern applications.
SSH RFC4253	The secure shell (SSH) transport layer protocol [12]	Secure Shell (SSH) is a cryptographic network protocol that allows secure communication and remote command execution over TCP port 22. It encrypts all transmitted data using protocols like AES and supports public key authentication.

These standards guarantee that NetCommand maintains safety and promotes accessibility. They include guidelines to manage secure shell protocol, management/access of remote devices, correct identification of switches, ethernet communication, network loop prevention, and configuration of wireless networks on compatible switches.

REFERENCES

- [1] Office of Advocacy, “Frequently Asked Questions About Small Business 2023,” *SBA’s Office of Advocacy*, Mar. 07, 2023. <https://advocacy.sba.gov/2023/03/07/frequently-asked-questions-about-small-business-2023/>
- [2] T. Freed, “Top Challenges With Network Management,” *Prelude Services*, Aug. 19, 2019. <https://www.preludeservices.com/blog/top-challenges-with-network-management/>
- [3] “Network Administrator Job Description,” ECU Online Programs, [Online]. Available: <https://onlineprograms.ecu.edu/blog/network-administrator-job-description/>. [Accessed: 12-Feb-2025].
- [4] “Information Technology - Generalist,” Nova Scotia Community College (NSCC), [Online]. Available: <https://www.nscc.ca/programs-and-courses/programs/plandescr.aspx?prg=ITGE&pln=ITGENERAL>. [Accessed: 12-Feb-2025].
- [5] “Cisco Discovery Protocol Configuration Guide, Cisco IOS Release 15M&T - Secure Cisco Discovery Protocol [Support],” *Cisco*, Jun. 2016. <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-secure-cdp.html> (accessed Mar. 16, 2025).
- [6] IEEE Standard for Ethernet, IEEE Standard 802.3-2018, IEEE, 2018. [Online]. Available: <https://ieeexplore.ieee.org/document/8457469>
- [7] IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks, IEEE Standard 802.1Q-2018, IEEE, 2018. [Online]. Available: <https://ieeexplore.ieee.org/document/8403927>
- [8] IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Bridges, IEEE Standard 802.1D-2004, IEEE, 2004. [Online]. Available: <https://ieeexplore.ieee.org/document/1309630>
- [9] IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control, IEEE Standard 802.1X-2020, IEEE, 2020. [Online]. Available: <https://ieeexplore.ieee.org/document/9018450>
- [10] IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Standard 802.11-2020, IEEE, 2020. [Online]. Available: <https://ieeexplore.ieee.org/document/9363693>
- [11] J. Postel and J. Reynolds, “Telnet protocol specification,” RFC 854, Internet Engineering Task Force, May 1983. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc854>
- [12] T. Ylonen and C. Lonvick, “The secure shell (SSH) transport layer protocol,” RFC 4253, Internet Engineering Task Force, Jan. 2006. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc4253>

The authors acknowledge the use of ChatGPT in the preparation of this assignment for phrasing and proofreading.