



Senior Design Project in Electrical & Computer Engineering



Wi-Fi TISCOM- Wireless Access and Security

Cadet 1/c Mark Bruno

Advisor: LT Moyer

Sponsor: TISCOM

Project Background

The advent of wireless technology, both in the public and private sectors, has driven the Coast Guard to evaluate the risks and benefits of implementing wireless solutions, throughout the service service wide. Increased productivity, better communications, and easier access from anywhere, not just the desk where the computer normally is.

The recent explosive growth of wireless technology is based largely on the improving security standards. Despite the advances, unauthorized access is a major concern for the secure military infrastructure. User authentication, and intrusion defense are vital considerations for the Coast Guard to evaluate before attempting to move to wireless networking.

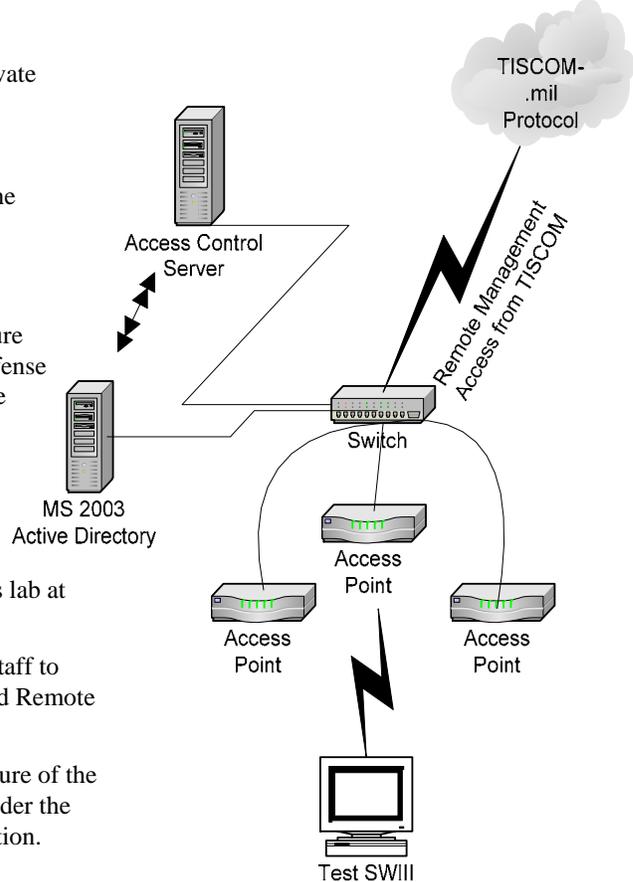


Project Work

- >Wire and Configure a wireless lab at CGA to TISCOM standards.
- >Work with TISCOM project staff to implement Active Directory and Remote Access Management.
- >Asses the current security picture of the Coast Guard network and consider the state after wireless implementation.

Project Plan

- >Identify Department of Homeland Security, Department of Defense, and TISCOM wireless computing requirements.
- >Deploy a Wireless solution onboard CGA with remote access to TISCOM.
- >Test and Adjust configurations to optimize service, administration, and intrusion protection.
- >Assess network vulnerabilities with and without the wireless solutions deployed.



Project Deliverables

- >Wireless test configuration, connected to TISCOM implementation of WLAN project. Support North and South Labs at TISCOM
- >Network Security Evaluation Report- To include current network security standards, current network security realization, wireless considerations, and recommendations to align current requirements and standards with implementation Coast Guard wide