Case Study Scenarios

Scenario 1: Network Segmentation in a University Computer Laboratory

The university maintains a large computer laboratory that is heavily utilized for programming, networking, and academic tasks. At present, all computers in the Faculty offices (5 PCs), Programming Lab (20 PCs), Networking Lab (15 PCs), and Library section (5 PCs) operate within a single flat network. This configuration results in unnecessary broadcast traffic, degraded performance, and unrestricted access across all connected devices. Faculty resources, in particular, are exposed and can be accessed without safeguards, presenting significant security risks. Compounding the issue, the wireless capability of the router has not been configured properly and continues to use its default settings. As a result, unauthorized individuals within range are able to connect freely, further compromising network integrity. The situation highlights the need for a more robust and secure infrastructure, one that incorporates VLAN segmentation for each area, router sub-interfaces to enable controlled inter-VLAN communication, and a properly configured wireless environment with authentication and encryption. Such an approach ensures efficiency, protects sensitive resources, and prevents unauthorized access.

Scenario 2: Securing Patient Data in a Small Hospital Network

A small community hospital relies heavily on its internal network to connect the Administrative Offices (10 PCs), Nurse Stations (6 PCs), and Patient Records Department (4 PCs), while also providing a Guest Wi-Fi area for visiting doctors (10 mobile devices). At the moment, all these groups share the same LAN, which puts patient confidentiality and system performance at risk. Administrative staff can unintentionally access sensitive patient information, while guests can connect to the same network that hosts critical medical devices. The absence of inter-VLAN routing makes it difficult for doctors to access records in real time, leading to delays in treatment and inefficiencies in data sharing. Furthermore, the router’s wireless feature has no encryption enabled, allowing anyone to connect freely. Students are asked to redesign this hospital network by applying VLANs to isolate each department, configuring router sub-interfaces for secure inter-VLAN communication, and implementing secure wireless access with strong authentication and encryption.

Scenario 3: Protecting Transactions in a Coffee Shop with Free Wi-Fi

A local coffee shop provides free Wi-Fi for customers while also depending on its network to process payments and manage operations. Currently, the same network is shared by POS terminals (2 devices), the Manager's Office computer (2 PCs), the Staff Wi-Fi for employees (3 devices), and the Guest Wi-Fi for customers (up to 15 devices during peak hours). Because everything runs on a flat network, sensitive transactions from POS terminals are exposed to the same environment used by guest devices, raising the risk of data interception. The lack of inter-VLAN routing prevents the Manager's Office from securely accessing sales data from the POS system. In addition, the router's wireless settings still use the default SSID and weak password, making the system vulnerable to unauthorized access. Students must analyze this case and propose a new design that separates POS, Management, Staff, and Guest networks into VLANs, implements inter-VLAN routing for required communication, and configures the router's wireless feature with secure SSIDs and strong encryption.

Scenario 4: Departmental Isolation in a Government Office

A municipal government office manages several important departments, including the Mayor's Office (4 PCs), Finance (8 PCs), Records (6 PCs), Human Resources (4 PCs), and IT Support (3 PCs). At present, all devices across these departments are connected to a single network segment, creating performance problems and exposing confidential files to unauthorized access. For example, HR employees are able to see finance-related files, and Records staff can unintentionally interfere with IT systems. Meanwhile, the Mayor's Office cannot efficiently access records since no inter-VLAN routing is in place, which hinders legitimate collaboration between departments. The router's wireless feature is left unprotected, allowing visitors within the building to connect to the internal LAN without restriction. Students are tasked to create a secure and efficient design by assigning VLANs for each department, enabling router sub-interfaces for controlled inter-VLAN routing, and configuring router-based wireless access to ensure secure connectivity for internal staff while restricting outsiders.

Scenario 5: VLAN Implementation in a Small Business Startup

A small IT startup company operates four divisions: Development (12 PCs), Human Resources (3 PCs), Accounting (3 PCs), and Marketing (4 PCs), plus several laptops and mobile devices connecting wirelessly (about 5 devices). All employees currently share one unsegmented network, which results in bandwidth issues and creates security risks. Developers consume large amounts of bandwidth for builds and testing, which slows down Marketing's ability to share files and conduct online meetings. HR and Accounting also face problems because confidential payroll and employee data are accessible on the same LAN used by developers. The absence of inter-VLAN routing makes collaboration between HR and Accounting inefficient, while the router's wireless configuration remains unchanged from default, allowing unauthorized users to connect easily. Students must evaluate this situation and propose a proper network design that assigns VLANs to each division, uses router sub-interfaces for controlled communication, and configures secure router wireless access to protect the company's sensitive resources.