Table of Content

Car Dealership Overview

Project Overview

This project aims to design a computer network for a car dealership. The network must support operations in four sales offices, two financial processor offices, a service area, and a reception area. The network will include computers, printers, and a server to manage customer appointments, sales history, and payments. The design must ensure that all devices communicate efficiently, considering that not all printers and computers may be Wi-Fi-enabled.

Computer Hardware Overview

The devices that we will need for the car dealership are:

- 7 PC (4- sales office, 2 - finance office, 1 - reception area)
- 2 Laptops (2 - for service in garage)
- 2 switches
- 1 server
- 1 router
- 2 printers (1 for the sales office shared, 1 for the service area to print service orders)

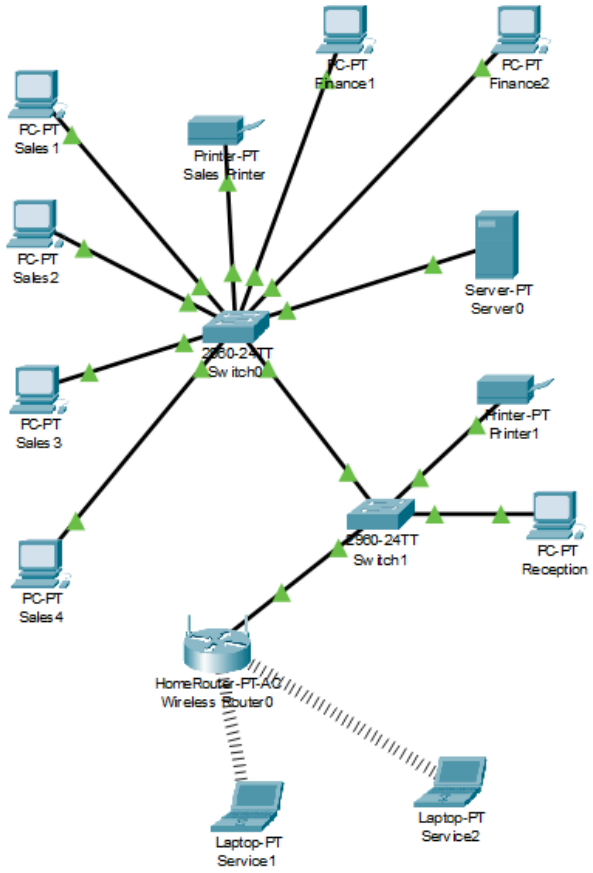
Printer Overview

HP - OfficeJet 8015e Wireless All-In-One Inkjet Printer

Category	**Feature**	**Details**
Key Specs	Print Speed (Color/Mono)	18 ppm
	Output Tray Capacity	60 sheets
	Touch Screen	Yes
Features	Automatic Document Feeder (ADF)	35 sheets
	Two-Sided Printing	Automatic

	Tray Capacity	225 sheets
Connectivity	Printer Connectivity	Wi-Fi, HP Smart, AirPrint
Scanner	Type	Flatbed
	Resolution	Up to 1200 x 1200 dpi
Fax	Integrated Fax	Yes
Paper Info	Supported Sizes	Letter, Legal, Envelope, Card, Photo

Network design



IP address details

The network address scheme will use a class B network.

- IP Segment: 196.168.0.0
- IP Subnet Mask: 255.255.0.0
- IP default gateway: 196.168.0.1

Device	**IP Address**	**Description**
Router	196.168.0.1	Default Gateway
PC 1	196.168.0.2	Sales1
PC 2	196.168.0.3	Sales2

PC 3	196.168.0.4	Sales3
PC 4	196.168.0.5	Sales4
PC 5	196.168.0.6	Reception
PC 6	196.168.0.7	Finance1
PC 7	196.168.0.8	Finance2
Laptop 1	196.168.0.9	Service1
Laptop 2	196.168.0.10	Service2
Printer 1	196.168.0.11	Sales printer
Printer 2	196.168.0.12	Printer1
Server	196.168.0.13	Server
Switch 1	196.168.0.14	Switch 1
Switch 2	196.168.0.15	Switch 2

Pricing information

Item	Price per item	Units need	Total cost
HP - Envy Desktop with Windows 11 Pro - Intel Core i5 - 16GB DDR4 Memory - 1TB SSD	$699.99	7	$4,899.93
Lenovo - IdeaPad 1 15.6" Full HD Touchscreen Laptop - Ryzen 7 5700U with 16GB Memory - AMD Radeon Graphics - 512GB SSD	$499.99	2	$999.98
HP - Officejet 8015e Wireless All-In-One Inkjet Printer	$159.99	2	$319.98

Linksys - Atlas 6 Wi-Fi 6 Router AX3000 Dual-Band Wi-Fi Mesh Wireless Router	$239.99	1	$239.99
Linksys - 16 Port Gigabit Unmanaged Network Switch	$79.99	2	$159.98
Server	$4500.00	1	$4,500.00
Cables	$250.00	12	$3,000.00
		Grand Total	$14,119.86

Car Dealership Security Strategy

Physical Layer Security:
This layer focuses on the physical protection of the network structure. One of the important steps is ensuring that our network remains secure. We will minimize risks and establish access controls.

Possible Threats:
Possible hazards at the physical layer include unauthorized access to network devices and physical damage to the network. Attackers intending to harm parts of our network pose a significant danger and can cause the loss of essential company data or disrupt network operations.

Strategy Proposed:
We will implement physical controls such as locking cabinets for network devices and restricting access to critical areas. This will ensure that only authorized personnel can interact with the equipment. Constant video surveillance will provide visibility into sensitive areas, such as the server room, while inventory management will help track hardware and prevent theft. Maintaining a regular inventory log will aid in tracking assets and preventing loss.

Network Layer Security:
This layer governs the routing and management of traffic across the network.

Possible Threats:
Dangers at this layer include unauthorized access, IP spoofing, and DoS attacks. The main goal of attackers is to gain access to the network, steal confidential information, impersonate others, and manipulate company services.

Strategy Proposed:
We will implement VLAN segmentation to secure specific areas of the network and reduce the risk of potential attacks. Additionally, a firewall will be installed to filter traffic within the network and prevent unauthorized access or DoS attacks.

Application Layer Security:
This layer is critical because it directly interacts with the user. At this layer, services such as browsers, email clients, and other applications operate, making it particularly vulnerable to malware, phishing attacks, and data breaches.

Possible Threats:
This layer is exposed to phishing attacks, malware infections, and web attacks like SQL injection or XSS, which can lead to the loss or exploitation of sensitive information.

Strategy Proposed:
We recommend installing and regularly updating antivirus software. A Web Application Firewall (WAF) will protect web applications against threats such as SQL injection and XSS.

Data Layer Security:
Protecting data within our network is essential. For the office, securing data from intruders and preventing its loss is critical.

Possible Threats:
Unauthorized access and data theft are primary threats at the data layer. Confidential information within the office network could be exposed, leading to severe consequences for the firm.

Strategy Proposed:
We will implement AES-256 encryption to secure data and use TLS to protect data during transmission. A backup system will be established to prevent data loss, and a Role-Based Access Control (RBAC) system will restrict access based on employee roles, adding additional protection.

Security Tests of the Car Dealership

Security Test for Physical Layer

Securing the physical layer requires limiting physical access to devices and continuously monitoring for unauthorized access. Switch logs should be consistently reviewed, and switches and routers must be placed in secure locations. For the server, physical access should be tightly controlled to prevent unauthorized manipulation.

To further enhance security, the company's security policy should include constant system monitoring for suspicious activity, isolating vulnerable network segments, and creating regular backups of critical data.

Security Test for Network and Applications Layer

According to our topology, devices such as switches connect computers, printers, and servers of a car dealership's respective departments of sales, finance, and service. A wireless router for laptops in the service department, a centralized server to store information, computers, printers

This topology has potentially dangerous areas, such as the network having no segmentation, making it vulnerable to external attacks that would allow an attacker to move freely throughout the network. The system can also be exposed to viruses, such as unpatched software default configurations on routers and switches. Moreover, it is worth protecting sensitive data by encrypting it.

At the network layer, switches are vulnerable to MAC address flooding and ARP spoofing. Setting strong passwords for routers is crucial to prevent unauthorized access. Laptops and

PCs may be exposed to malware or phishing attacks, and installing antivirus programs on all computers and laptops is strongly recommended.

To test the health of our network, we recommend using various tests, including passive and active scanning, penetration testing, and vulnerability scanning. For passive scanning, we will use programs such as Wireshark and Nmap to leave the network untouched and find potentially vulnerable areas in ports, services, etc. We use the Nessus program for active scanning, allowing us to eliminate problems with weak configurations and programs. Penetration testing and its utilities, such as Metasploit, will be able to create a simulation of actual attacks that will allow us to assess possible threats more deeply. For a more detailed vulnerability scanning, we will use a utility like OpenVAS, and thanks to it, we will be able to find potential weak points among devices in the whole network.

If we talk in more detail about the use of these programs and utilities, we can deduce the following. Nmap will identify open ports and services on switches, routers, and PCs, while Wireshark will analyze traffic for suspicious activities such as ARP spoofing. Nessus and OpenVAS will uncover missing patches and insecure configurations, and Metasploit will be used for penetration testing.

To accurately mitigate the risk, we will secure the switches by configuring their ports to protect them from MAC flooding. DAI should be enabled to stop ARP spoofing. For the wireless router, the master password should be changed to a stronger password to prevent unauthorized access to our network through the router. It should also use the WPA3 encryption system. To secure the server and the information stored in it, we will configure it with AES-256 encryption and Role-based access control (RBAC). As for the rest of the devices, we can only mention the correct configuration of their passwords and constant support of antivirus programs.