[Github Repository](https://github.com/barkhadD/smart-iot-farm)

# Introduction

The integration of Internet of Things (IoT) technology in agriculture or *smart farming* is transforming the traditional farming practices. IoT refers to the network of interconnected sensors and devices that collect and exchange data over the internet thus enabling the real-time monitoring and control​ [1]. In agriculture this will mean that embedding farms with sensors for the soil moisture, climate, livestock trackers and automation systems to optimize the operations. These advancements will promise to enhance the productivity and resource the efficiency. For example the precision agriculture using IoT has shown improvements in the crop yields and also reduced the resource wastage​ [[8]](https://www.hashstudioz.com/blog/from-waste-to-wealth-how-iot-sensors-help-farmers-save-water-fertilizer/#:~:text=Empowering%20farmers%20to%20envision%20a,smarter%2C%20more%20sustainable%20agricultural%20future). This report will present a detailed network design for a smart farm scenario. The design is developed using the GNS3 network simulator. The aim of it is to demonstrate how a robust network infrastructure can support IoT devices on a farm, ensuring reliable connectivity and security for critical agricultural data.

# Research on IoT in Agriculture

## IoT and its Role in Modern Agriculture

IoT (Internet of Things) is a term used for the model where physical things and devices are mounted with computing and network connectivity, therefore, they can both send and receive data. This is possible with IoT in agriculture through the combination of devices and sensors that are installed together to form a so-called "smart" network that can work alone by collecting data and even manage the responses by itself [1]. Farming IoT devices include examples like soil moisture sensors, weather stations, GPS-connected farm machinery, livestock wearables, smart irrigation controllers, and IP cameras. Soil moisture probes, weather stations, GPS-enabled farm machinery, livestock wearables, smart irrigation controllers, and surveillance cameras are representative of the IoT devices used on farms.

The precision agriculture sector, which IoT technology supports, is a method that adjusts farming decisions according to very specific information. The use of sensors in the fields to determine soil conditions and plant health is enabling the irrigation and fertilization to be done in the best way for each crop zone [2]. IoT-based weather stations, moisture sensors provide automation of the irrigation systems. Thus, the crops are given water only at required times. Livestock sensors could also detect animal behavior and vital signs thus leading to better herd management and early disease diagnosis [2]. The coupling of these systems via farm networks enables operations like greenhouse climate control, automated feeding, and remote surveillance of fields.

## Wireless Network Features and Constraints for IoT

A farm mostly has IoT devices that are connected wirelessly because it has to span wide areas outdoor without the need for extensive cabling. In agricultural IoT, various wireless technologies are typically used and most of them have different features and limitations. For example Wi-Fi is frequently used near farm buildings when data rate is high as For example streaming IP camera footage of a range limited to a few hundred meters [8]. However, LoRaWAN is the one that guarantees the long-distance and low power connection which can cover several kilometers, and it is the best choice for a large number of sensors distributed in a wide area field [8].

Range and coverage are of utmost significance during the installation of wireless networks within a farm. The open-field settings allow for signals to propagate, but objects like trees, hills, or greenhouses could attenuate wireless signals. Far-off farms usually have poor internet backhaul connections because infrastructure is limited [4]. Even in the local scenario, physical barriers like crop canopies or metal walls could distort Wi-Fi signals [4]. This mirrors the need for accurate antenna placement or the employment of technologies such as LoRa or external high-gain antennas capable of penetrating obstacles. Bandwidth needs range from low, where small telemetry packets are all that simple sensors send, to significantly higher throughput for video streams or heavy telemetries such as drone data. Wireless networks need to be designed to handle the peak data rates and latency-sensitive applications.

Another constraint is power. Many IoT sensors run on battery or solar power in the field. Protocols like LoRaWAN and Zigbee are optimized for low energy usage, while a Wi-Fi can be power-hungry. In all cases, reliability is crucial. Farmers depend on these networks for timely alerts (e.g., a greenhouse temperature spike), so the network must be resilient to outages. Strategies such as using redundant communication paths or edge computing can reduce the connectivity issues​ [[4]](https://bigdata.cgiar.org/three-major-obstacles-for-iots-in-agriculture/#:~:text=3,Cloud).

## Security Concerns and Vulnerabilities in IoT Network

Many IoT devices have limited processing power and also lack the robust security controls. It has been shown that security measures are often lagging behind the rapid deployment of IoT gadgets. The reason is that many devices cannot easily receive the firmware updates/patches which causes persistent vulnerabilities​ [[5]](https://xml.jips-k.org/full-text/view?doi=10.3745/JIPS.03.0178#:~:text=increasing%20exponentially,analyzed%20the%20most%20common%20security). For example a vulnerable sensor or camera could be compromised and used to infiltrate the broader network or leak sensitive data such as farm operational data or video feeds.

Data security is an important concern in the smart agriculture because of the volume and value of data collected from sensors and cameras. Making sure the privacy and integrity and secure transmission of this data is important so as to prevent the unauthorized access and breaches​ [[8]](https://www.data-alliance.net/blog/agriculture-iot-wireless-technologies-for-ag-internet-of-things/#:~:text=In%20the%20ever,breaches%2C%20and%20potential%20cyber%20threats). Key security considerations include the encryption of data communication e.g., using WPA2/WPA3 for Wi-Fi networks, or AES encryption in Zigbee/LoRaWAN, authentication of devices to prevent spoofing, and network access control. To handle these risks, modern network design principles recommend segmenting IoT devices onto separate network segments or VLANs isolated from the core business network [[7]](https://www.infosecinstitute.com/resources/management-compliance-auditing/vlan-network-chapter-5/#:~:text=Network%20segmentation%20with%20virtual%20local,to%20perform%20their%20daily%20tasks).

## Commercial and Environmental Impacts of IoT Adoption

Investing in IoT technology in agriculture has the commercial benefits and environmental implications. From a business standpoint the data-driven approach of IoT can greatly improve the operational efficiency and crop yield. By applying water and fertilizer and pesticides only as needed and in precise amounts, the farmers can reduce the waste and input costs while maintaining or improving output. Traditional farming often suffers from inefficiencies and studies indicate that roughly 30% of the irrigation water is lost because of evaporated or not using it and up to 50% of the fertilizers ends up polluting the waterways rather than aiding crops [[8]](https://www.hashstudioz.com/blog/from-waste-to-wealth-how-iot-sensors-help-farmers-save-water-fertilizer/#:~:text=The%20stark%20reality%20is%20that,to%20water%20scarcity%20and%20pollution). Such waste directly erodes profitability and harms the environment through water scarcity and pollution. IoT-based solutions directly address these issues, for example smart irrigation systems use the soil moisture sensor data to irrigate only when and where necessary, preventing overwatering.

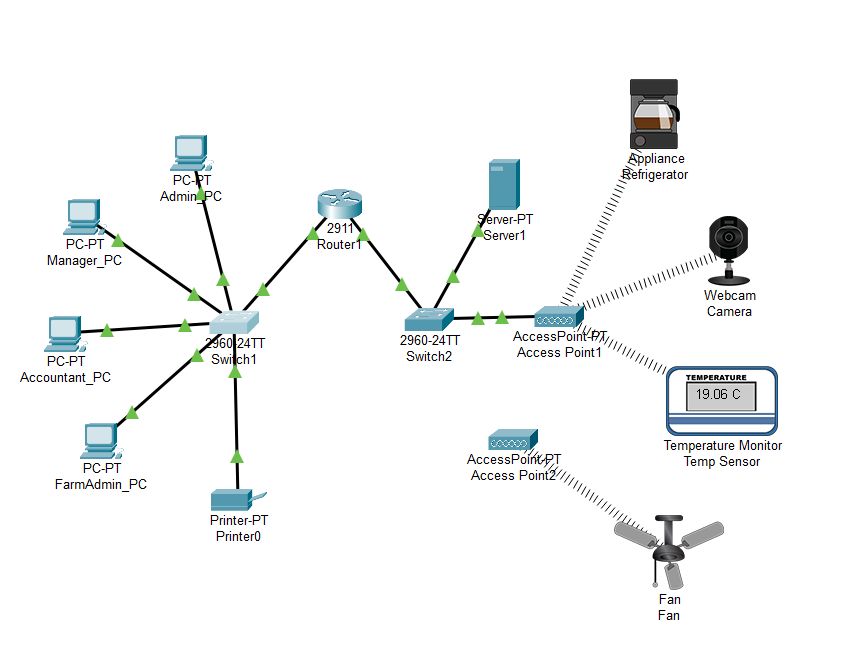
IoT can lower the labor and operating costs. Automation like autonomous tractors can reduc the manual workload. Energy savings are realized by optimizing pump and equipment usage. Even though implementing IoT infrastructure can require a high amount of upfront investment the long-term returns justify the cost. In many cases, farmers see a return on investment within just 1–3 years due to the combined savings from water, energy, and labor, coupled with higher revenues from better yields​ [[9]](https://smartwatermagazine.com/blogs/justin-nichols/economic-benefits-iot-driven-smart-irrigation-systems#:~:text=Although%20the%20initial%20investment%20in,costs%2C%20and%20increased%20crop%20yields). Additionally, external factors like government incentives for precision agriculture and sustainability initiatives can subsidize the adoption of IoT, further improving the commercial case​ [[9]](https://smartwatermagazine.com/blogs/justin-nichols/economic-benefits-iot-driven-smart-irrigation-systems#:~:text=Although%20the%20initial%20investment%20in,costs%2C%20and%20increased%20crop%20yields).

# Network Design and Implementation

## Design

The network that is designed in Cisco Packet Tracer for the diversified farm requirement and includes a market garden with greenhouses, a pick-your-own (PYO) field, a farm shop, a café and office facilities. The network has the support for the variety of connected devices which is including the office and the management desktops for staff, point-of-sale terminals, smart refrigerators, environmental control systems, the IP cameras and the kitchen devices. The network is able to handle both the wired and also the wireless connections using the VLAN segmentation to improve the security and the efficiency.

* A segmented star topology is implemented. The topology is centered around a core switch in the main building.
* A single edge router connects the farm’s network to the Internet.
* The router connects to a core switch, which distributes connections to different areas.
* VLANs are used to logically separate traffic.
* VLAN 10 is for the office network with the subnet 192.168.10.0/24, VLAN 20 is for PoS devices with the subnet 192.168.20.0/24, VLAN 30 is for IoT sensors with the subnet 192.168.30.0/24, and VLAN 40 is for public WiFi with the subnet 192.168.40.0/24.



## Security

To enhance security following measures were taken:

1. Unused switch ports were disabled to prevent the unauthorized physical access.
2. Port security was implemented to restrict MAC address connections which is ensuring that only authorized devices can connect.
3. Access control lists (ACLs) were used to limit the inter-VLAN communication and also to prevent the unauthorized access between the networks.
4. SSH was configured on the router to secure that the remote access thus replacing the Telnet.
5. A dedicated management VLAN was created to isolate the switch and the router configurations from general traffic.
6. DHCP snooping was then enabled to prevent the rogue DHCP servers from disrupting the network.

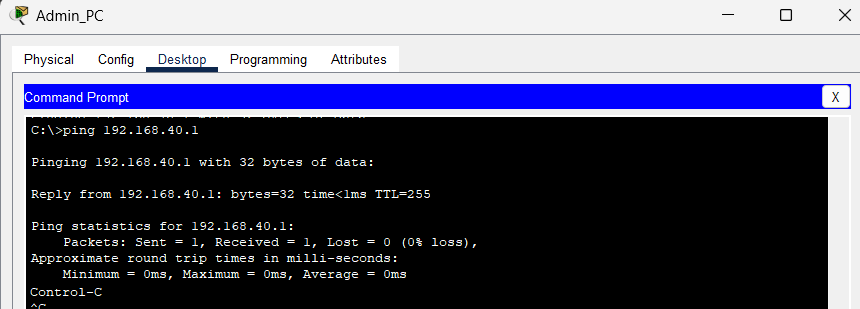
## Performance

Performance was optimized by:

1. Enabling Spanning Tree Protocol (STP) to prevent the loops using EtherChannel for the link aggregation to improve the bandwidth
2. Applying Quality of Service (QoS) policies to prioritize the critical traffic such as the PoS transactions and security cameras.
3. Wireless performance was improved by assigning the non overlapping channels and implementing the WPA2 security for the encryption.

## Connectivity Testing

* Once the network was configured then the connectivity tests were performed to verify functionality.
* Each PC was tested to ensure it received an IP address via DHCP and could communicate with the gateway.
* Pings were conducted between devices within the same VLAN to confirm local connectivity.
* Inter-VLAN communication was tested by pinging across VLANs to validate the router’s routing functionality.
* Internet connectivity was checked by pinging an external address, ensuring the router was forwarding traffic correctly.
* The wireless devices were verified for stable connectivity to the appropriate access points, and security measures such as ACLs were tested to ensure unauthorized communication was blocked.



# Analysis and Evaluation

## Analysis

In Cisco Packet Tracer, the Router1, Switch1, Switch2, access points and end devices like the PCs, PoS terminals and IoT devices were added. Wired connections were configured using the Ethernet cables. Trunk links were established. The wireless connectivity was configured for IoT devices and the public WiFi. The VLANs were created on Switch1 and Switch2 and ports were assigned. The trunk connection to the router was set to allow all VLANs. On Router1, sub-interfaces were created for each VLAN with dot1Q encapsulation, and appropriate IP addresses were assigned. DHCP pools were configured for each VLAN to automatically assign IP addresses to connected devices. Access points were mapped to the correct VLANs and SSIDs were assigned for wireless connectivity. Connectivity was verified by testing the pings between devices in the same VLAN, testing inter-VLAN communication, and verifying DHCP assignments on Router1.

## Evaluation

The network design provides the efficient VLAN segmentation for security and performance and provides the scalable architecture for supporting both the wired and the wireless connectivity. Automated DHCP is also provided for the simplified device management and the isolated guest WiFi to prevent the unauthorized access to internal resources. Security enhancements such as disabling unused ports, implementing port security, enabling ACLs for access restriction, using SSH for secure management, and applying DHCP snooping contribute to protecting the network against potential threats. Performance improvements through Spanning Tree Protocol, EtherChannel link aggregation, QoS policies, and optimized wireless settings ensure efficient data transmission and reliable connectivity across all farm operations.

Areas for improvement include the following:

1. Adding a firewall for enhanced security.
2. Implementing a secondary router for redundancy.
3. Enabling centralized network monitoring for fault detection

# Conclusion

In analyzing the solution, we found that the network has achieved a strong balance of performance and the security for the smart farm scenario. The strength of the networks are many and lie in the segmentation, scalability, and alignment with best practices for example limiting the attack surface via network isolation and using the automation like DHCP for the easy management. The security optimizations then further strengthen the network by restricting the unauthorized access and improving overall resilience. The network enables the farm to harness the IoT capabilities from automated greenhouse management to the real time inventory tracking. This translates into the commercial gains and also the environmental benefits.

# References

[1] Omnitron Systems. *“IoT in Smart Agriculture Networks.”* Omnitron Blog, 2023. Overview of IoT and its applications in agriculture, including definitions and examples of smart farming use cases.

[2] Omnitron Systems. *“What is IoT, and How Does it Fit into Agriculture?”* (Section in *IoT in Smart Agriculture Networks*). Explains the concept of IoT in agriculture and discusses various sensor and device applications on farms.

[3] Hardesty, George. *“Agriculture IoT: Wireless Technologies for Ag Internet of Things.”* Data-Alliance Blog, Nov. 5, 2023. Details common wireless technologies (Wi-Fi, Bluetooth, LoRaWAN, NB-IoT, Zigbee, etc.) used for IoT in agriculture and their characteristics (range, power, bandwidth).

[4] Owade, Atula. *“Three major obstacles for IoTs in agriculture.”* CGIAR Big Data in Agriculture Blog, Oct. 11, 2018. Describes challenges such as poor connectivity in rural farms and how innovative solutions (e.g., TV white spaces, drones) can overcome them.

[5] Kim, Hee-Hyun, and Jinho Yoo. *“Analysis of Security Vulnerabilities for IoT Devices.”* **Journal of Information Processing Systems**, vol. 18, no. 4, 2022, pp. 489–499. Academic study highlighting common IoT device security issues (e.g., lack of timely patching) and the growing number of vulnerabilities as IoT expands.

[6] Data Alliance. *“Challenges and Future Outlook”* (section of *Agriculture IoT: Wireless Technologies for Ag IoT*). Emphasizes the importance of data security in smart agriculture, noting the need to ensure privacy, integrity, and protection of IoT-collected data.

[7] Infosec Institute. *“VLAN Network Segmentation and Security.”* (Olzak, Tom, 2021). Explains VLAN segmentation fundamentals and notes that proper network segmentation can reduce attack surfaces and limit unauthorized access in networks.

[8] Hashstudioz (Shivam Rathore). *“From Waste to Wealth: How IoT Sensors Help Farmers Save Water & Fertilizer?”* Feb. 16, 2024. Provides statistics on resource waste in traditional farming and improvements achieved with IoT sensors (e.g., 15% yield increase, 20% less water usage).

[9] Nichols, Justin. *“The economic benefits of IoT-driven smart irrigation systems.”* Smart Water Magazine, Aug. 9, 2024. Discusses cost savings and return on investment for IoT-based irrigation, noting that farmers often see ROI within 1–3 years due to water savings, labor reduction, and yield gains.