Section 3

Timothy Udumula

Department of Information Technology, University of Maryland, Baltimore County

CYBR 624 (Spring 2025): Cybersecurity Project

Dr. Behnam Shariati

May 13, 2025

Abstract

The current integration of Internet of Things (IoT) devices into Small Office Home Office environments raises security challenges. The IoT devices are limited due to resource limitations, computing power, and a design that is not security-centric. This paper proposes a policy-driven technical solution framework that includes the NIST Cybersecurity Framework to maximize the security posture of the SOHO IoT network. The paper issues strategies which include network segmentation via VLANs, implementation of standard access control lists (ACLs), centralized DNS filtering, monitoring, logging, and employing automated update mechanisms. Zero-trust principles are embedded in the proposed framework to limit unauthorized access and traffic between networks. The prescribed solution is deemed adaptable, lightweight, and carries minimal administrative oversight in the SOHO IoT network. This methodology is built upon the NIST CSF core functions: Govern, Identify, Protect, Detect, Respond, and Recover.

Keywords: Zero-Trust architecture, IoT, VLAN, ACL, DNS filtering, security policy, SOHO, NIST CSF.

Table of Contents

Lists of Abbreviations

Abbreviation	Definition
ACL	Access Control List
AP	Access Point
CSF	Cyber Security Framework
DNS	Domain Name System
IoT	Internet of Things
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
LAN	Local Area Network
NIST	National Institute of Standards and Technology
SOHO	Small Office Home Office
VLAN	Virtual Local Area Network

Glossary of Terms

Term	Definition
ACL	A rule-based policy list is implemented on a router to allow or deny traffic.
AP	Networking device which allows networking devices to connect to a wired device over the air.
CSF	A guideline set enabled by NIST
DNS	A system that resolves human-readable names to IP addresses
IoT	Devices in a network that are embedded with sensors and technologies that communicate over the internet.
IDS	A network solution that detects malicious traffic
IP	32- or 128-bit address of a device to communicate over the network.
IPS	A network solution that detects and prevents malicious traffic
LAN	The term is designated for networks in a smaller broadcast domain.
NIST	An agency that develops guidelines such as the CSF.
SOHO	Term refers to small area networks that are limited in network structure.
VLAN	Logical partition of ports on a switch to separate segments in a network.

3. Methodology

3.1 Overview

The Internet of Things devices are being enabled in many enterprise spaces daily. The ease of use, availability, and affordability are why they are preferred in the enterprise or production spaces. As discussed in sections 1 and 2, several issues exist about the rampant usage of the Internet of Things. The technology evolves every day, and the need to find fast solutions to the ever-changing information technology environment requires suitable solutions. Hence, the Internet of Things is considered a preferred solution to the demands of the Information Technology realm, and they have become a part of daily life (Szymoniak et al., 2025). However, several drawbacks exist as the current Information Technology is concerned with the security implementation, and notably, the Internet of Things devices certainly possess security flaws. Most IoT devices have not been specifically designed to tackle the ever-growing security needs. The IoT devices are being implemented in many sectors, from Information Technology to Healthcare. This is a concern since the IoT devices do not offer extensive security measures (Okereke et al., 2024), and the design of the IoT devices is comparatively straightforward in contrast with more complex devices in the enterprise spaces with more computing capacity (Kabir et al., 2023).

This paper will discuss the implementation and methodology/ model of the topic mentioned in section 1. The paper primarily concerns the security of small enterprise structures called Small Office Home Office. Small Office Home Office environments are relatively small compared to other enterprise structures because the network design in a SOHO environment is not sophisticated. SOHO environments consist of a layer-3 switch or a router to switch to the end host network design; however, in refined network architectures, the network footprint is more prominent, consisting of numerous firewalls, IDS, IPS, routers, APs, end hosts, and security appliances. An in-house admin team would be responsible for the core infrastructure in a sophisticated enterprise architecture. However, the underlying responsibility in SOHO environments is not massive enough to enact a full-scale admin team. Moreover, the technical prowess of the SOHO environment employees may be questionable when handling security problems. A comprehensive policy-driven technical framework is required for an environment such as SOHO networks to maintain a security posture against IoT device issues.

3.2 Methodology/Model

The current model combines the prescribed NIST Cybersecurity Framework (CSF) to solidify compliance and structured risk management. The NIST CSF section embarks on the introduction by delving into the core functions (Govern, Identify, Protect, Detect, Respond, Recover) to address IoT security needs. The proposed model briefs the technical details, including VLAN segmentation of the networks, Access Control Lists (ACLs) for layered traffic control, and Pi-hole DNS application device for the framework for the function in an example network SOHO structure. Moreover, the proposed section also signifies the importance of automatic updates and zero-trust policies to solve the issue of the number-of-days vulnerabilities.

The NIST CSF for this model is chosen for the wide range of use; it is adaptable to several environments, and the SOHO environment is no exception. Delving more into the NIST CSF, the framework, which is suitable for a wide range of enterprise networks or organizations, is a suitable option for the adaptability it offers because NIST CSF provides a hierarchical structure of rules and guidelines for employing security in enterprise environments. From Figure 1, the core functions of the NIST Cybersecurity Framework 2.0 (2023) are Identify, Protect, Detect, Respond, and Recover. Since SOHO networks are increasing in the small-scale enterprise structure around the world and availability of a comprehensive policy-driven technical solution is unavailable, the proposed structure which incorporates the discussed framework into the SOHO architecture will be beneficial to the small-scale SOHO enterprises because the integration of IoT devices, and employing the principles can provide a flexible solution to the problem discussed in section 1, and provides a simple structure-based approach which secures the conventional and smart devices of the network infrastructure.

The network architecture of an SOHO environment is often trivial, as detailed in Figure 2, with an internet gateway and the rest of the network described as a single Local Area Network or in the same broadcast domain; the architecture is prone to several issues concerning security implementation. Table 1 shows the Functions of NIST CSF, which are mapped to the SOHO environment discussed previously. First, observing the functions of the NIST CSF, we conclude by identifying and classifying the assets in the SOHO environment because identifying the assets in an environment is crucial to determining what to protect. Second, once we lay the foundation to identify the assets, we follow the second core function of the NIST CSF: Protect. This section details classified or segmented access, which is enabled by implementing Access Control Lists rules to minimize communication across networks and employ the least privilege. Third, we follow the third core function of the NIST CSF: Detect, in this section we employ Domain Name System parameters in the SOHO environment, it is common that the names are resolved through an external DNS in SOHO environments, this does not control the ingress and egress traffic flow, hence, a DNS threat logging system is implemented through the Pi-hole application device. This solution enables monitoring and logging of suspicious queries or potential malicious domains initiated by IoT devices or external actors. Fourth, we follow the fourth core function of the NIST CSF: Respond. In this section, the parameters mentioned, such as ACL and DNS policies, are implemented automatically through the configured rules. SOHO environments are smaller than complex enterprise networks, and configuring sophisticated regulations and guidelines may hinder the smaller networks from adapting. Hence, policy and guideline configurations on a compact scale are appreciated on the network, which minimizes human intervention for manual rejection or approval for traffic that flows in the SOHO environment. Finally, we follow the fifth core function of the NIST CSF: Recover. This section is significant in the framework proposed. In an adverse event, it is vital to retrieve the data that is regularly backed up. In a small environment such as SOHO, it is crucial to contain data, configuration, policy, regulations, and guidelines in an uncorrupted segment. For instance, in the proposed environment, we include and save the system-critical back-ups such as ACL and VLAN configurations. Moreover, we initiate automated cron-jobs on the device firmware and policy backups this can ensure that reular patches are applied and the devices are running current version of firmware updates, and reduces manual execution of updates, this aids in reducing the numbe of days vulnerability which is a trivial factor when dealing with IoT devices in a SOHO network.

3.2.1 Technical Implementation, VLAN

From Figure 1, the network segmentation is applied following the NIST CSF framework. Network segmentation is crucial to parse unnecessary traffic between segmented networks. Defining a borderline between networks reduces blast radius during adverse events (Magara & Zhou, 2024). Moreover, excessive traffic, such as broadcast messages, which consume network traffic, will be contained in the respective broadcast domain within the segmented networks. Figure 1 portrays the VLAN segmentation, VLAN 10 for administrative networks, VLAN 20 for user devices, VLAN 30 for IoT devices, and VLAN 40 for backup systems. This zero-trust-based

VLAN segmentation limits lateral movement between segmented networks for SOHO environments.

3.2.2 Technical Implementation, ACL

The router in the SOHO would enact the ACL configurations (Kokila and K, 2024), we implement ACL lists on the router and apply them to the router subinterfaces, this would limit the traffic flow between VLAN segmentation where only the Admin is given the highest priority of access to the VLAN 20, 30, and 40, however the VLAN communication to the Admin VLAN 10 is restricted. Considering the sophistication, only the extended ACL list is not employed in the SOHO environment, and the priority to implement secure functions and not exceed the sophistication is a significant task in SOHO environments; thus, the standard ACL would suffice the requirement for VLAN traffic restrictions. Figure 1 details the running configuration on the SOHO environment router, enabling ACL.

3.2.3 Technical Implementation, DNS setup

In this section, the implementation of DNS filtering is observed. The framework utilized in this paper addresses the core function Detect, and the implementation of DNS filtering plays a vital role in solidifying the security in small-scale environments such as SOHO environments. Considering the limitations of the SOHO environment and the limitations of the IoT devices in the SOHO environment, we implement a compact but powerful solution to monitor and log traffic that flows in the SOHO network. For this solution, we considered Pi-Hole DNS filtering. The Pi-hole, which is located between the switch and router, resolves all the DNS queries, and the Pi-hole will act as the primary point of contact for all the VLANS, users, and devices in the network. We induce necessary policies in the devices to maintain a blocklist and allowlist to allow and reject traffic based on the configured policies. Moreover, this enables centralized control over the network. In the current framework, the devices in the network resolve their DNS requests through the IP address 192.68.1.2, which is the static address for the Pi-hole server, and Pi-hole allows a user-friendly web management interface for less sophisticated environments such as SOHO. This solution reduces the impact of IoT devices being utilized as attack vectors in the SOHO network by rejecting malicious traffic based on pre-configured policies in the SOHO policy. Finally, Pi-hole maintains curated logs for the traffic flow, which will help the network administrator maintain a secure posture.

3.2.4 Technical Implementation, Automatic Update Mechanism

Updates are an integral part of maintaining proper security posture in the network, devices often require updates, and this situation is significant in SOHO IoT networks, moreover, in the current network the VLAN segmentation, ACL rules, DNS filtering would aid the security posture, however, updates are necessary for the devices in the VLANs, since the focus of the research questions begs the plausible solution for the SOHO IoT environment, it is essential to consider the SOHO environment and derive a plausible solution which would lead to automatic update mechanism, because in a SOHO environment there may be several IoT devices in existence, maintaining the updates on each device would consume time and effort, however, issuing automatic updates would streamline the process for the environment. This mechanism is achieved by utilising the infrastructure of IoT devices. This step includes issuing cron-jobs on the devices so that they can be scheduled for future automatic updates, and this step ensures minimal human intervention, which is a primary concern in the SOHO environment (Bakhshi et al., 2024), as the employees may range at various technical levels. Hence, such an automatic mechanism would be sufficient for a small-scale environment such as the SOHO IoT environment. Figure 3 shows the automatic update mechanism script running without human intervention during non-production hours. This script is not ideal concerning the sophistication that can be induced, such as forwarding the logs to a subdirectory. However, this illustration is included to demonstrate that the automatic mechanism of the IoT devices can be trusted and performed in the SOHO IoT environment.

3.2.5 SOHO IoT Policy-driven Technical Implementation

The following policy-driven technical recommendation is tailored for the SOHO IoT environment network described in the section, offering a lightweight, scalable, resilient, concise, and adaptable policy that would suffice a small-scale environment such as the SOHO IoT environment. This section details the policy recommendation following the NIST CSF core functions. They are as follows: First, the Segmentation of the Network in accordance with NIST core functions, Identify and Protect, the segmentation of the network to reduce unnecessary traffic is implemented by VLANs in the order of VLAN10 (Admin), VLAN 20 (Users), VLAN 30 (IoT), and VLAN 40 (Backups). Lateral movement of traffic between VLANs is prohibited except for the Admin's access to the VLANs. For instance, Admin access to IoT devices in VLAN 30 to verify the update mechanism from section 3.2.4. Second, implementation of

Access Control in accordance with NIST core function Protect. In addition to the network segmentation into unique VLANs, the implementation of Access Control is crucial in the SOHO IoT networks, considering that the inclusion of standard ACL is deployed to minimize sophistication. For instance, IoT devices in VLAN 30 cannot authorize user devices in VLAN 20. However, they are permitted to access the outbound Internet through the network gateway. Third, implementation of DNS filtering in accordance with NIST core function, Detect and Protect. DNS resolution is critical in a SOHO IoT environment. In this solution, the implementation of a lightweight, cost-effective solution, such as a DNS sinkhole in VLAN 10, causes the devices in the consecutive VLANs to resolve their queries through 192.168.1.2 in VLAN 10. The pre-configured policies in the Pi-hole will monitor and automatically deny or allow specified traffic, and will aid the admin for potential log analysis if necessary. Fourth, implementation of the Automatic Update Mechanism in accordance with NIST core function, Recover. Regular updates are essential for proper security posture in the network, from Figure 5, we observe an illustration of the IoT device updates that do not require frequent human intervention, thus IoT devices in VLAN 30 are patched regularly and firmware versions should be reviewed by the Admin once a month, similarly, inter-VLAN devices should follow a similar update schedule to maintain homogeneous security posture (El Jourhari, 2022). Fifth, implementation of Zero-Trust in accordance with NIST core function, Govern and Respond. Devices in the network should not be trusted by default. Hence, sufficient access should be granted to carry out productivity tasks. Devices in VLAN 30 do not require admin access to perform assigned tasks. Hence, access should be limited concerning their function. The pre-configured ACL and VLAN segmentation work in coordination to enforce policies across the network. Finally, the prescribed policy recommendation is suitable for the discussed SOHO IoT network, where the policy-driven technical solution takes advantage of the existing lightweight network architecture by understanding the technical limitations of the IoT devices, which will secure the network through the policy based on the NIST CSF framework fulfilling the core function requirements such as Gover, Identify, Protect, Detect, Respond and Recover.

3.3 Results

The prescribed approach to resolve the research question from section 1 is that the topic aim to cover the aspects of the security problems associated with the implementation of IoT devices, continual updates, segmentation of the IoT network in an SOHO environment, improper access control, and will focus on resolving by proposing a framework that includes policy and technical solutions that would help streamline the security and privacy in IoT systems. Reflecting on the policy observation and the research question, we aim to compare the network environment before and after implementing the policy-driven technical solution. Table 2 shows several things: First, the network segmentation has succeeded in restricting inter-vlan traffic, which was inconsistent before the policy implementation. Second, central DNS filtering, monitoring, and logging are conducted from the Admin VLAN of the network, which increases the security posture as the Internet Service Provider previously maintained it. Third, Access Control Lists were enforced to confine unauthorized traffic movement between VLANS, in contrast to the open and implicit communication between VLANs prior to the implementation of the policy. Fourth, the policy implementation has switched from a manual update mechanism to an automatic update mechanism, which reduces the burden of manually installing updates. Fifth, a real-time monitoring solution is enabled by using the installed network DNS solution, which enables filtering, monitoring, and logging. Sixth, the SOHO IoT network benefits from a standard conscience and lightweight policy (Alkhurayyif & Weir, 2017), which enables enhanced security measures for the network. Finally, the network posture has moved from a reactive-based approach to a proactive approach through preconfigured policy implementation based on the zero-trust principles. Thus, the prescribed policy implementation secures a plausible solution to the research question from section 1 by inducing a policy-driven technical solution that considers the limitations of the SOHO-based IoT networks, however, leverages the lightweight solutions to implement robust security measures to tackle the malicious attempts against the insecure network architecture.

References

Szymoniak, S., Piątkowski, J., & Kurkowski, M. (2025). Defense and Security Mechanisms in the Internet of Things: A Review. *Applied Sciences*, *15*(2), 499. https://doi.org/10.3390/app15020499

Okereke, G. E., Mathew, D. E., Ukeoma, P. E., Uzo, B. C., Umaru, A. A., & Dibiaezue, N. F. (2024). IoT device security and network protocols: A survey on the current challenges, vulnerabilities, and countermeasures. *International Advanced Research Journal in Science, Engineering, and Technology*, 11(7). https://doi.org/10.17148/IARJSET.2024.11701

Kabir, M. a. A., Elmedany, W., & Sharif, M. S. (2023b). Securing IoT devices against emerging security threats: challenges and mitigation techniques. *Journal of Cyber Security Technology*, *7*(4), 199–223. https://doi.org/10.1080/23742917.2023.2228053

Toward a Secure Firmware OTA Updates for constrained IoT devices. (2022, September 26). IEEE Conference Publication | *IEEE Xplore*. https://ieeexplore.ieee.org/document/9922087

Kokila, M., & K, S. R. (2024). Authentication, access control and scalability models in Internet of Things Security–A review. *Cyber Security and Applications*, *3*, 100057. https://doi.org/10.1016/j.csa.2024.100057

Magara, T., & Zhou, Y. (2024). Internet of Things (IoT) of smart homes: privacy and security. *Journal of Electrical and Computer Engineering*, *2024*, 1–17. https://doi.org/10.1155/2024/7716956

Bakhshi, T., Ghita, B., & Kuzminykh, I. (2024). A review of IoT firmware vulnerabilities and auditing techniques. *Sensors*, *24*(2), 708. https://doi.org/10.3390/s24020708

A Large-Scale empirical study on the vulnerability of deployed IoT devices. (2022, June 1). *IEEE Journals & Magazine | IEEE Xplore*. https://ieeexplore.ieee.org/document/9259111

Readability as a basis for information security policy assessment. (2017, September 1). IEEE Conference Publication | *IEEE Xplore*. https://ieeexplore.ieee.org/document/8090409

The NIST Cybersecurity Framework (CSF) *2.0. (2023). https://doi.org/10.6028/nist.cswp.29*

Appendix A

Tables and Figures

Table 1

NIST CSF Functions mapped to SOHO IoT

NIST CSF Function	SOHO IoT Security Application
Identify	Asset classification and VLAN segmentation
Protect	ACL implementation for segmented access
Detect	Monitoring and logging of DNS threats
Respond	Blocking policies initiated by ALC and DNS
Recover	Recovery of scheduled firmware and policy backups

Note. This table describes the mapping structure used in section 3 of the paper. The NIST CSF functions are categorically mapped to the respective SOHO IoT security applications.

Table 2

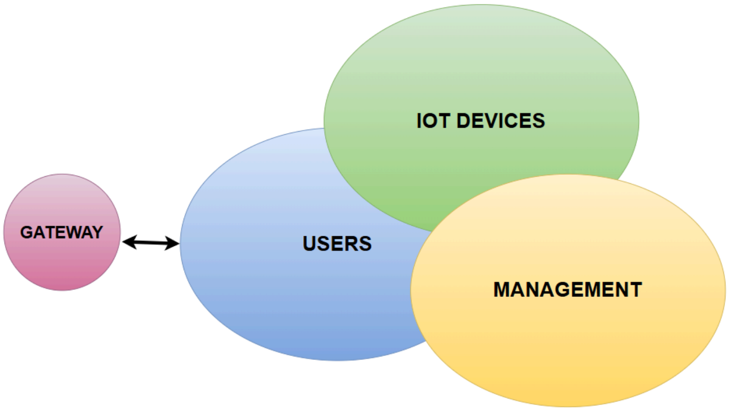
Comparison of the SOHO setup to the proposed NIST CSF functions

Attribute of Security	Default SOHO Setup	Proposed Framework
Network Architecture	Single-subnet network	VLAN segmentation based on roles
DNS	ISP responsibility	Dedicated Admin VLAN responsibility
Access Control	Unauthorized traffic flow	Standard ACL implementation blocks unauthorized traffic
Update Mechanism	Manual and infrequent	Automatic update mechanism
Monitoring	Minimal	Real-time monitoring with a network DNS solution
Policy Function	Absence of formal structure	Deployment of SOHO IoT policy
Security Architecture	Reactive approach	Proactive approach

Note. This table illustrates how the proposed SOHO IoT security framework improves upon typical small office setups by aligning each technical enhancement with key NIST CSF functions.

Figure 1

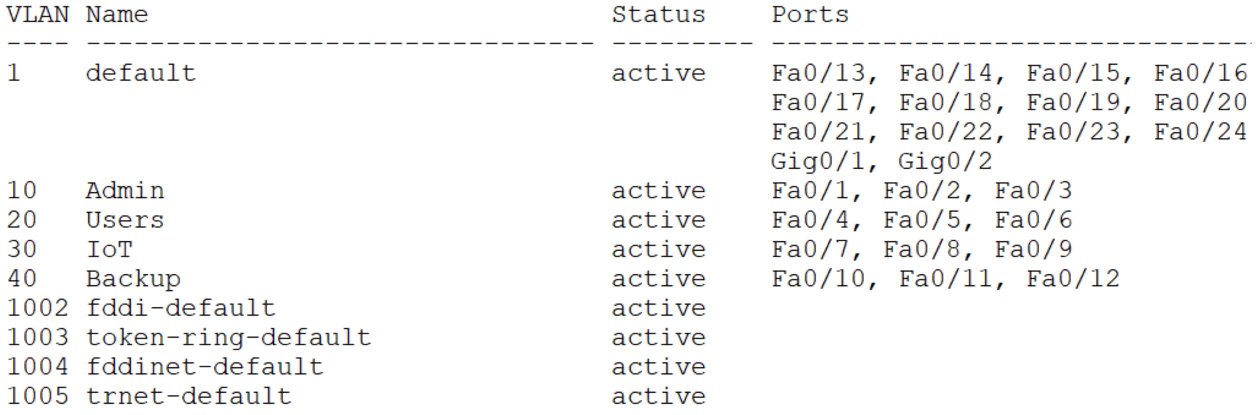
Illustration of Default SOHO IoT Network



Note. Illustrated network of the default SOHO IoT networks that do not employ concise security solutions

Figure 2

VLAN Segmentation of the Proposed Network Architecture

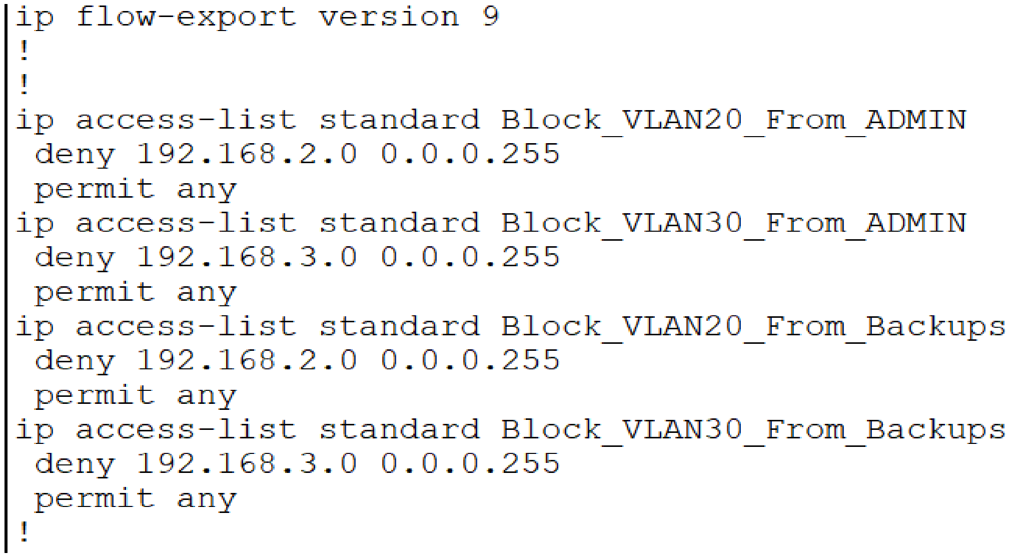


```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   Admin                            active    Fa0/1, Fa0/2, Fa0/3
20   Users                            active    Fa0/4, Fa0/5, Fa0/6
30   IoT                              active    Fa0/7, Fa0/8, Fa0/9
40   Backup                           active    Fa0/10, Fa0/11, Fa0/12
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Note. A configuration screenshot of a Cisco switch details the VLAN segmentation of the VLANs based on roles, VLAN10-Admin, VLAN20-Users, VLAN30-IoT, and VLAN40-Backup**.**

Figure 3

ACL implementation between VLANs 10-40

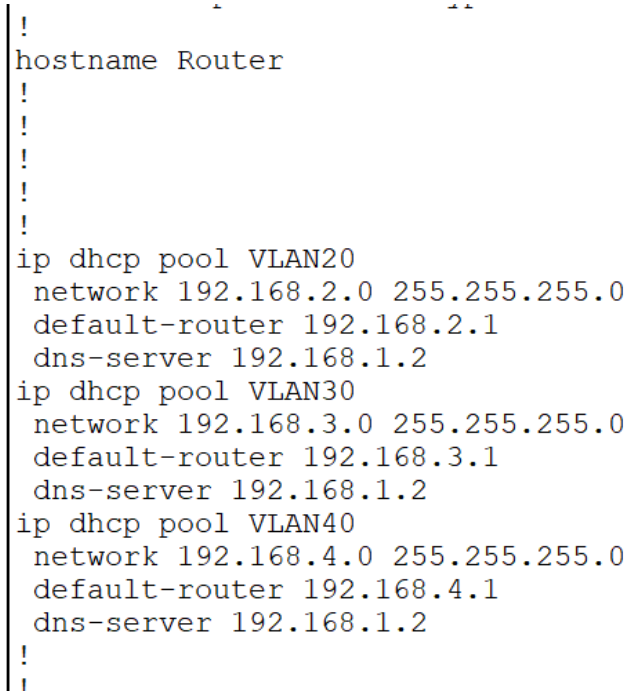


```
ip flow-export version 9
!
!
ip access-list standard Block_VLAN20_From_ADMIN
 deny 192.168.2.0 0.0.0.255
 permit any
ip access-list standard Block_VLAN30_From_ADMIN
 deny 192.168.3.0 0.0.0.255
 permit any
ip access-list standard Block_VLAN20_From_Backups
 deny 192.168.2.0 0.0.0.255
 permit any
ip access-list standard Block_VLAN30_From_Backups
 deny 192.168.3.0 0.0.0.255
 permit any
!
```

Note. A configuration screenshot of a Cisco router details the ACL implementation of the SOHO IoT network.

Figure 4

DNS Implementation through Pi-hole

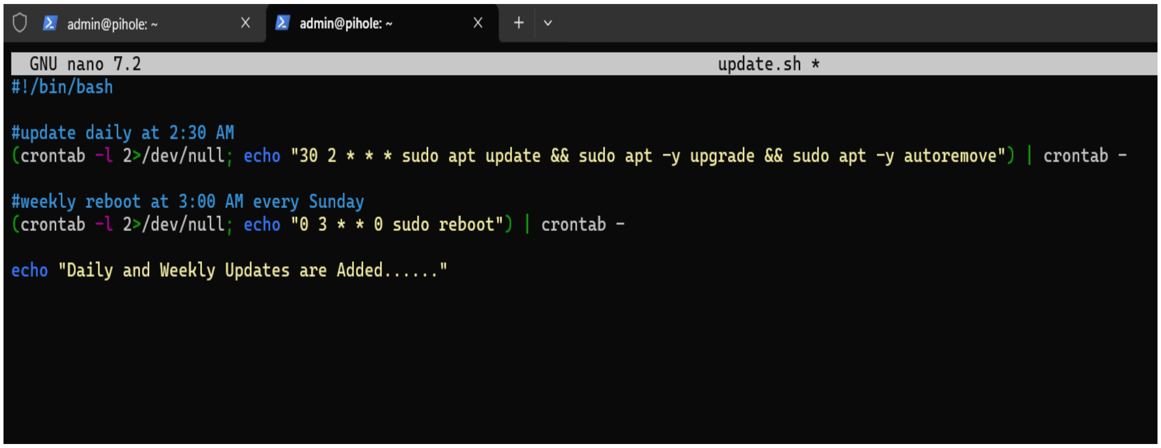


```
!
hostname Router
!
!
!
!
!
ip dhcp pool VLAN20
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
 dns-server 192.168.1.2
ip dhcp pool VLAN30
 network 192.168.3.0 255.255.255.0
 default-router 192.168.3.1
 dns-server 192.168.1.2
ip dhcp pool VLAN40
 network 192.168.4.0 255.255.255.0
 default-router 192.168.4.1
 dns-server 192.168.1.2
!
!
```

Note. The devices in the respective VLANS 20-40 will send their DNS queries to the 192.168.1.2 DNS solution.

Figure 5

Automatic Update Mechanism Illustration



```
#!/bin/bash

#update daily at 2:30 AM
(crontab -l 2>/dev/null; echo "30 2 * * * sudo apt update && sudo apt -y upgrade && sudo apt -y autoremove") | crontab -

#weekly reboot at 3:00 AM every Sunday
(crontab -l 2>/dev/null; echo "0 3 * * 0 sudo reboot") | crontab -

echo "Daily and Weekly Updates are Added......"
```

Note. The screenshot presented represents the application of automated update mechanism possibility in all IoT devices from VLAN 10 and VLAN 30.