DEMONSTRATING CYBERSECURITY IN PRACTICE

VLAN Implementation for NIST Cybersecurity Framework Education

By Drew E. Brown

Abstract

As cybersecurity threats continue to increase, there is a growing need for effective cybersecurity education and training that develops practical skills. This paper demonstrates hands-on, experience-based learning is critical for building real-world cybersecurity capabilities. An implementation of virtual local area networks (VLANs) to segment traffic is presented as a tangible example to teach foundational access control protections aligned with the "Protect" function of the NIST Cybersecurity Framework. The paper provides a step-by-step demonstration of configuring VLANs on commercial networking devices to create isolated virtual networks. Relevant standards including 802.1Q VLAN tagging are explained in detail during the technical discussion. The VLAN implementation is mapped to specific categories and subcategories of the NIST Framework to illustrate the connection between theoretical cybersecurity guidance and applied practices. This paper serves as a recommendation for how hands-on cybersecurity exercises can incorporate into academic curriculums to better prepare students for professional challenges. The paper demonstrates the direct experience of building protections is an effective educational approach that reinforces security concepts.

ODU School of Cybersecurtiy – Norfolk, Va
CYSE697 Master’s Project | August 15, 2023

I. Introduction

As cyber and physical security continue converging in an increasingly interconnected world, cyber threats facing individuals and organizations are continuously growing in scale and sophistication. The rapid expansion of networked devices and systems brought on by the Internet of Things (IoT) revolution has created new vulnerabilities even as it has enabled innovation. Major data breaches across sectors demonstrate the need for enhanced cyber resilience and unified security strategies. The National Institute of Standards and Technology's (NIST) Cybersecurity Framework provides guidelines for managing risk by identifying security requirements, modeling threats, and implementing protections. While NISTs framework does not focus on home networks, it states that the guidance is “intended to be useful to companies, government agencies, and not-for-profit organizations regardless of their focus or size.” (2) This indicates the framework can provide a solid cybersecurity foundation for homes as well; it simply needs to be adapted for the wider populace.

The focus of this paper is around the “Protect” function of the framework by providing hands-on cybersecurity education through configuring virtual local area networks (VLANs). The goal is to make technical protections tangible through practical application. Firsthand cybersecurity education is critical for developing real-world skills and academia could improve student preparedness through practical laboratory examples like configuring VLANs to reinforce security principles. Using the NIST Cybersecurity Framework standards enables cross referencing of technical documentation and applied real-world applications. This demonstrates how organizations can evaluate and improve their cybersecurity readiness through proactive testing frameworks and adaptive risk mitigation further reinforcing students for professional engagements.

II. NIST Cybersecurity Framework Overview

The National Institute for Science and Technology develops ongoing framework advancements to best protect and securely design critical infrastructure security implementations through a risk-based approach. NIST’s first iteration of *Framework for Improving Critical Infrastructure Cybersecurity V1.0* was first published 12Feb2014. This 40-page document consists of a 3-part framework: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. A second revision was produced by NIST throughout 2017 and 2018 and released as Version 1.1. Version 1.1 incorporates community and business sector feedback during the first 5 years of their Cybersecurity Framework use which refines, clarifies, and enhances the subject matter of Version 1.0. As stated by NIST, the Framework “intends to provide direction and guidance to those organizations – in any sector or community – seeking to improve cybersecurity risk management.” (“Getting Started | NIST”) (3) It should be noted that NIST has just recently announced a Cybersecurity Framework V2.0 on August 08, 2023. Version 2.0 is still under development, but it is important to recognize that best practices are in constant flux. (4)

a. The Framework Core

The Framework Core will support the primary focus of this paper when and is a structured approach to managing cybersecurity risk that is adaptable to different organizations and environments. More specifically, the “Protect” function will be demonstrated in this paper through the implementation of virtual local area networks (VLANs) using various physical networking components. As an overview, “the

Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors." ("Cybersecurity Framework FAQs Framework Components | NIST") (2) The Framework Core consists of four components: Functions, Categories, Subcategories, and Informative References.

Framework Core Elements:

Functions - There are five continuous high-level cybersecurity functions that aim to organize basic cybersecurity activities. These functions assist organizations in communicating their missions' needs and capabilities to help realize where cybersecurity and management risks persist.

- Identify - Develop an organizational understanding to understand and begin cybersecurity risk management.
- Protect – Define available safeguards to ensure or improve delivery of critical services.
- Detect – Understand current activities in place to identify occurrences of cyber events. Improve as necessary.
- Respond – Establish standard operating procedures which defines activities of action during a cyber event.
- Recover – Ensure routine back-ups are available and assess abilities to maintain resilience and restore capabilities.

Categories - Each subdivision contains multiple cybersecurity outcomes grouped into categories. These categories provide deeper insights "into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities." (2, 3) The below lists example categories across 4 of 5 functions:

- Asset Management (AM - Identify)
- Identity Management Authentication and Access Control (IM/AC - Protect)
- Threat Intelligence (TI - Identify)
- Data Security (DS - Protect)
- Incident Response Planning (IRP - Respond)

Subcategories – This further breaks down categories into more-specific outcomes which enables deeper research and analysis identification among various technical documentation to support informative references selection. (2)

- Physical devices and systems within organization are inventoried. (AM - Identify)
- Physical access to assets is managed and protected. (IM/AC – Protect)
- Data-at-rest is protected. (DS – Protect)
- Notifications from detection systems are investigated (IRP – Respond)

Informative References – this compiles all applicable references gathered during information gathering phase from existing standards, guidelines, and practices that supports the pathways towards achieving the desired stakeholder outcomes with this Cybersecurity Framework.

- Center for Internet Security Critical Security Controls (13) - CIS Controls
- Information Systems Audit and Control Association – Control Objectives for Information and Related Technologies (14) - ISACA COBIT 5
- Security and Privacy Controls for Information Systems and Organizations (5) - NIST SP 800-53 Rev. 5

In summary, the Framework Core provides a methodology to assess, benchmark and classify cybersecurity activities across 5 key functions. Following the core focus identifications, the Framework employs tiers to evaluate maturity and profiles to determine gaps to enable risk-based approach to cybersecurity. (2, 3)

b. The Framework Implementation Tiers

Framework Implementation Tiers outline 4 tiers that represent degrees of risk management from Partial (Tier 1) to Adaptive (Tier 4). The tier classifications provide a mechanism for organizations to evaluate and improve cybersecurity risk management approaches over time. (2)

Implementation Tiers - 4 levels describing increasing cybersecurity risk management:

- Tier 1 (Partial) – An Informal, reactive, and focuses on discrete activities. Cyber risk management occurs in an ad-hoc manner that “may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.” (2) In other words, organizational cybersecurity risk management is not an organizational-wide program. External participation is minimal or largely non-existent. Implementation of cyber education and training from top to bottom, bottom to top, is necessary.
- Tier 2 (Risk Informed) – Is a risk-based approach with management approved policies, and planned practices, however, these practices and policies may not be organizational-wide. An awareness campaign may exist at the organizational level but managing the risks associated with cyber-domain interactions is largely unmitigated. External participation is moderate and “the organization collaborates with and receives some information from other entities.” (2)
- Tier 3 (Repeatable) – Denotes a well-defined program incorporating cybersecurity into operational risk processes. Consistent program implementation is observed across the organization and receives regular updates based on the organization's risk quantifications. It is verifiable that “senior cybersecurity executives and non-cybersecurity executives communicate regularly regarding cybersecurity risk.” (2) External participation is prioritized, and collaborative information sharing occurs between the organization and other organizations.
- Tier 4 (Adaptive) – The highest tier organization can adapt dynamically based on predictive indicators identified from their cyber risk management program and their engaged partners.

> Advanced data analytics and automation is utilized and deployed to better understand "the relationship between cybersecurity risk and organizational objectives." (2) External participation occurs in a leadership capacity which establishes proactive communication within and outside of an organization. Real-time and near real-time communications assist with decision-making.

In summary, the Implementation Tiers enable organizations to benchmark and mature their cybersecurity activities to manage risk and achieve objectives. The Tiers range from basic hygiene to highly adaptive programs. The tiers act as aids to improve and enable cybersecurity risk management programs within organizes of all sizes.

c. The Framework Profile

Framework Profiles intend to capture an organizations current state (Current Profile) and their target state (Target Profile) to identify gaps better align their cybersecurity efforts with measurable objectives that combine a wide range of informative references. These profiles align "the Functions, Categories, and Subcategories with [their specific] business requirements, risk tolerance, and resources." (2) Comparison of current and target profiles will assist the business with identifying and closing security gaps with a defined action plan created by the organization; "This Framework does not prescribe Profile Templates, allowing for flexibility in implementation." (2)

III. The Basics: Benefits to Creating VLANs

Virtual local area networks are typically associated with enterprise networks. These enterprise configurations boast of several benefits to enterprise organizations which enables businesses to adopt robust network security frameworks through segmentation, traffic management, Quality of Service (QoS), network design flexibility, cost savings, ease of troubleshooting, and Internet of Things device isolation. The security benefits from creating VLAN's can also be applied in a personal home network.

Network segmentation through VLAN's enable increased security and privacy. Security improvements occur by isolating general network traffic from administrative network traffic. The privacy improvements enable local, purpose-built servers/PC's keep their sensitive data private from other guest connections or IoT connections which notoriously lack up-to-date security patches.

Virtual local area network configurations enhance traffic management by significantly reducing broadcast traffic, such as Address Resolution Protocol (ARP) requests, which arise when new network connections are established or when one device seeks the Media Access Control (MAC) address of another. Instead of experiencing network broadcast flooding, which is common in expansive networks, traffic can be segmented into designated VLANs. This segmentation not only streamlines network management but also boosts traffic efficiency. By confining broadcast traffic to its specific VLAN, administrators can minimize superfluous traffic in other network segments.

Additionally, network management is improved enabling troubleshooting improvements. Issues can be isolated to specific VLANs, making it easier to identify and resolve network configuration issues.

Equipment moves, additions, and changes become simpler, moving physical equipment or cabling is no longer required as the administrator can simply reassign VLAN membership.

Cost savings is another benefit to VLAN implementations. VLANs can reduce the need for expensive network upgrades or additional hardware. Instead of adding more physical networks, one can segment the existing network virtually.

Network policies are more straightforward to manage in environments configured with VLANs. Each VLAN can have tailor-made network policies, allowing for precise control. Quality of Service (QoS) can be adjusted and prioritized based on typical network traffic patterns. Furthermore, access controls can be set at the VLAN level, ensuring that specific network traffic resources are either allocated or restricted based on policy requirements.

In summary, VLANs provide a logical segmentation that makes networks more secure, efficient, flexible, and easier to manage compared to traditional flat networks. Virtual Local Area Networks are a foundational building block for modern network design. With these benefits in mind, let’s explore their implementations across a local network.

IV. Advanced 802.1Q-based VLANs: Implementing Virtual Local Area Networks

a. VLAN Identification and Tagging

The 802.1Q tag header is a standard protocol defined in the IEEE 802.1Q specification that is used in Ethernet frames to implement VLAN tagging. It consists of 32 bits that are inserted into the Ethernet frame between the source and destination MAC addresses. The 802.1Q tag contains several fields including the Tag Protocol Identifier (TPID), Priority Code Point (PCP), Drop Eligible Indicator (DEI). These fields are beyond the scope of my network configuration. One of the more important fields is the 12-bit Virtual Local Area Network Identification (VLAN ID) field that is inserted in the modified Ethernet frame/Wi-Fi packet. By inserting this 802.1Q tag header into Ethernet frames, managed switches and VLAN supported routers/Wi-Fi access points can identify which VLAN a particular frame belongs to. With this VLAN ID, the frame can be appropriately routed to maintain the segmentation and boundaries between different VLANs. (6)

The 12-bit VLAN ID field can represent values between 0 and 4095, allowing for up to 4096 distinct VLAN assignments. However, some values like 0 and 4095 are reserved for special uses and cannot be configured as normal VLAN IDs. The purpose of the VLAN ID field is to specify the unique identifier corresponding to the particular VLAN that a given frame within a packet is associated with. It enables network devices (managed switches and VLAN-supported routers/Wi-Fi access points) that process the frame to identify the configured VLAN membership of that frame and route the packet according to the policies and rules defined for that VLAN. This ensures that traffic is properly isolated and segmented. (6)

The tagging process of VLAN configurations involves several steps. First, network devices such as managed switches are configured to assign specific ports to certain VLANs. When an Ethernet frame enters a port that is defined as a tagged port for a particular VLAN, the switch inserts an 802.1Q 4-byte tag header between source/destination MAC addresses including the proper VLAN ID for a specified VLAN into the data frame carrying the specific Ethernet frame. While beyond the scope of this paper, it should be noted that Internet traffic is packaged differently based its transmission medium; this means Ethernet frames are different from Wi-Fi packets due to their different tagging needs as the data frames/packets traverse networks. (6)

As a tagged frame/packet traverses the network, other switches and routers can read the 802.1Q tag and VLAN ID to determine how the frame should be handled according to the sending VLAN's network policies. When the frame reaches the destination port, if that port is configured as untagged for the destination VLAN, the 802.1Q tag is stripped from the frame before forwarding it to the end device. This overall VLAN tagging process ensures that traffic is appropriately segmented and isolated within the defined boundaries of each VLAN. It maintains the integrity of the virtual network divisions. One final note is the VLAN ID tag does not remain within ethernet frames for the duration of network traversal. Once the frame reaches its destination within the VLAN, the 802.1Q tag is removed and the end device receives the frame without the VLAN tag, as if it were on a regular ethernet network. (6)

b. VLAN Trunking and Links

Trunk links are connections between switches that carry traffic for multiple VLANs over the same physical link. Trunking allows VLANs to span across multiple switches since a single trunk link can transport frames for different VLANs by using VLAN tagging. Trunk links are configured by enabling trunk mode on the ports at both ends of the link. Trunking eliminates the need for dedicated links between switching equipment per VLAN by multiplexing traffic over shared links. This means that VLAN ID frames are the network segmentations preventing overlapping VLAN traffic in a shared or trunked link.

Network switches are configured with ports that can be defined as tagged or untagged for specific VLANs. As discussed previously, tagged ports add an 802.1Q header with the VLAN ID when forwarding frames from that VLAN. Untagged ports do not add the 802.1Q tag, for endpoints that don't support VLAN tagging. Untagged ports are primarily used to connect end devices like computers, printers, phones, etc., that don't understand VLAN tagging. Since untagged ports lack VLAN ID headers, they are not suitable for trunking. Traffic through these ports must be processed by a receiving host that understands the specific VLAN configuration; otherwise, it will be dropped from the network altogether. Trunk ports are configured to carry traffic for all allowed VLANs on a link, using tags to identify each VLAN. They enable communication between switches, maintaining VLAN information across the network.

The native VLAN is a concept related to trunk links. It is the default untagged VLAN for a trunk port. Traffic for the native VLAN does not receive an 802.1Q tag when traversing the trunk. This allows compatibility with legacy switches that don't understand VLAN tagging. Every trunk should have a native VLAN configured to properly transport untagged traffic.

VTP (VLAN Trunking Protocol) and DTP (Dynamic Trunking Protocol) are Cisco proprietary protocols that facilitate automatic configuration of trunk links between Cisco switches. They dynamically negotiate trunk settings to establish compatibility between linked switches. VTP also propagates VLAN information to synchronize VLAN IDs across switches.

c. VLAN Configuration and Management

Port assignment is a core aspect of VLAN configuration and involves assigning switch ports to specific VLANs. The purpose is to determine which devices belong to a VLAN based on which switch port they connect to. Network administrators configure the port-to-VLAN assignments using the command line or graphical management interface on the switches. Precise port assignments are crucial for segmenting devices into appropriate virtual networks.

VLAN creation is the process of defining and configuring new VLANs on switches. Each VLAN must be given a unique identification number and can also be assigned a descriptive name. The purpose of VLAN creation is to enable network segmentation by isolating devices and traffic into logical groups like departments or functions. The creation process is handled on switches and typically done by network administrators.

By default, VLANs operate in isolation from one another. Inter-VLAN routing enables controlled communication between VLANs when needed. This is accomplished by Layer 3 switches or routers that route traffic between VLANs based on IP addresses. Selectively allowing VLAN connectivity, rather than isolation, provides flexibility. The method of VLAN configuration also impacts network management. Static VLAN configuration offers precise control but can require extensive administrative effort. Dynamic VLAN configuration automates assignments based on policies to improve flexibility and reduce overhead.

V. Network Equipment Specifications

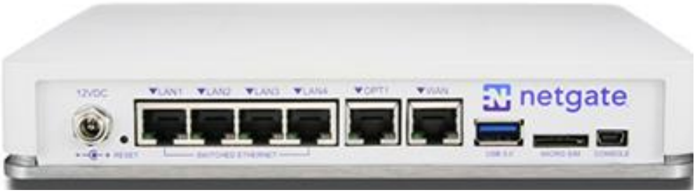
The Netgate 3100 Firewall appliance is specifically optimized for pfSense software. pfSense is an open-source firewall and router software distribution based on FreeBSD. This software provides a suite of Local Area Network/Wide Area Network (LAN/WAN) capabilities such as firewall, Virtual Private Network (VPN), routing, Dynamic Host Configuration Protocol (DHCP), Domain Naming Service (DNS), load balancing and several other network features. The software supports a web-based Graphical User Interface (GUI) for configuration and monitoring; depending on configurations is accessible from both LAN/WAN. This device also supports configuration through Secure SHell (SSH)/Command Line Interface (CLI) connections as well as console port connections. Management configurations for this network demonstration will take place over this firewall’s web GUI. Additionally, wide protocol support is leveraged – from IPv4, IPv6, VLANs, VPN protocols, etc. More hardware specifications are listed in the Netgate 3100 Specifications section. (7, 8, 9, 10)

The Netgear JGS516PE managed switch is a 16-port Gigabit Ethernet switch with all RJ45 ports for twisted pair connectivity. This device Supports layer 2 and basic layer 3 managed switch capabilities as well as provides 802.1Q VLAN support with up to 4096 VLAN IDs and 255 VLAN groups. Security features include access control lists, port security, and DHCP snooping. Management of this device occurs via web-browser GUI, CLI, or Simple Network Management Protocol (SNMP). The SNMP management occurs through vendor supplied software. Configurations for this network demonstration will take place over the switch’s web GUI. More hardware specifications are listed in the Netgear JGS516PE Managed Switch Specifications section. (11)

The TP-Link EAP225 Wi-Fi access point is a performant dual-band 802.11ac Wave 2 wireless access point suitable for small to medium business Wi-Fi deployments. It has a fast wireless throughput with a PoE-enabled compact form factor. This device supports 2x2 antenna array MIMO (multiple input, multiple output) with two spatial streams allowing for two independent spatial streams of data transmissions at the same time providing wireless coverage up to 5,000 square feet. This access point supports 16 BSSIDs per radio band for multiple SSIDs and supports up to 128 associated client devices. More hardware specifications are listed below in the TP-Link EAP225 Wi-Fi Access Point section. (12)

a. Netgate 3100 Firewall Appliance Specifications

Netgate 3100 Security Gateway (Front)



Netgate 3100 Security Gateway (Rear)

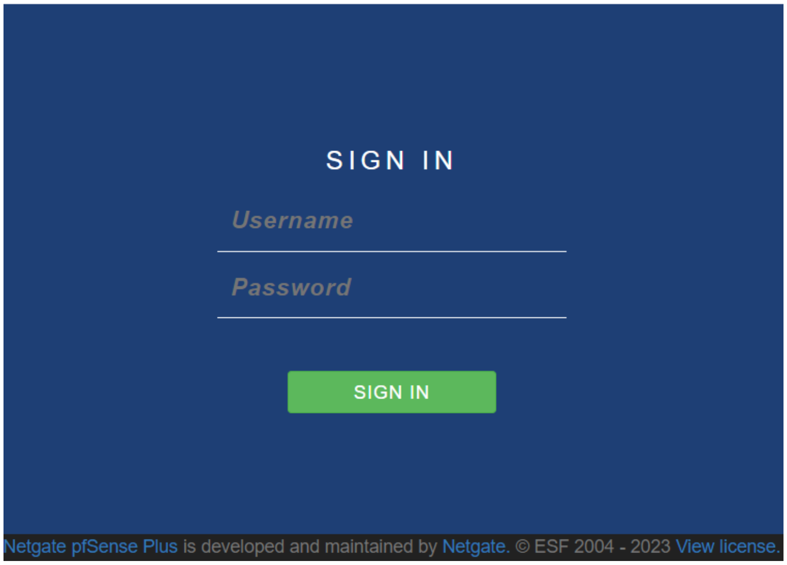
Hardware Specifications (7, 8, 9, 10):

Category	Description
CPU	ARM v7 Cortex-A9 @ 1.6 GHz with NEON SIMD and FPU
CPU Cores	Dual Core
Networking	• Two 1 Gigabit Ethernet Ports, configured as dual WAN or one WAN one LAN • 4-port 1 Gbps Marvell 88E6141 switch, uplinked at 2.5 Gbps to the third port on the SoC for LAN.
Storage	8 GB eMMC Flash onboard, upgradable to 32 GB M.2 SATA SSD

Category	Description
Memory	2-GB DDR4L
Expansion	2x M.2 ‘B’ key sockets (SSD, LTE) 1x M.2 ‘E’ key socket (2230 form factor) for WiFi / Bluetooth 1x miniPCIe (WiFi) microSIM
Console Port	MiniUSB (console cable included)
USB Ports	1x 3.0 port
LED	3 user-controllable full-color RGB LEDs
Enclosure	Desktop 1.56” tall x 7” deep x 8” wide
Form Factor	Standard mini-ITX 170mm x 170mm
Cooling	Passive (no fan)
Power	External ITE P/S AC/DC 100-240V, 50-60 Hz, 12V 3.33A, threaded barrel connector AC Inlet: IEC320-C14 (3 PIN) US Power Cord: NEMA 5-15P to IEC320-C13
Environmental	32°F (0°C) to 149°F (65°C)
Certifications	FCC, CE, RoHS, UL, IEC-60950

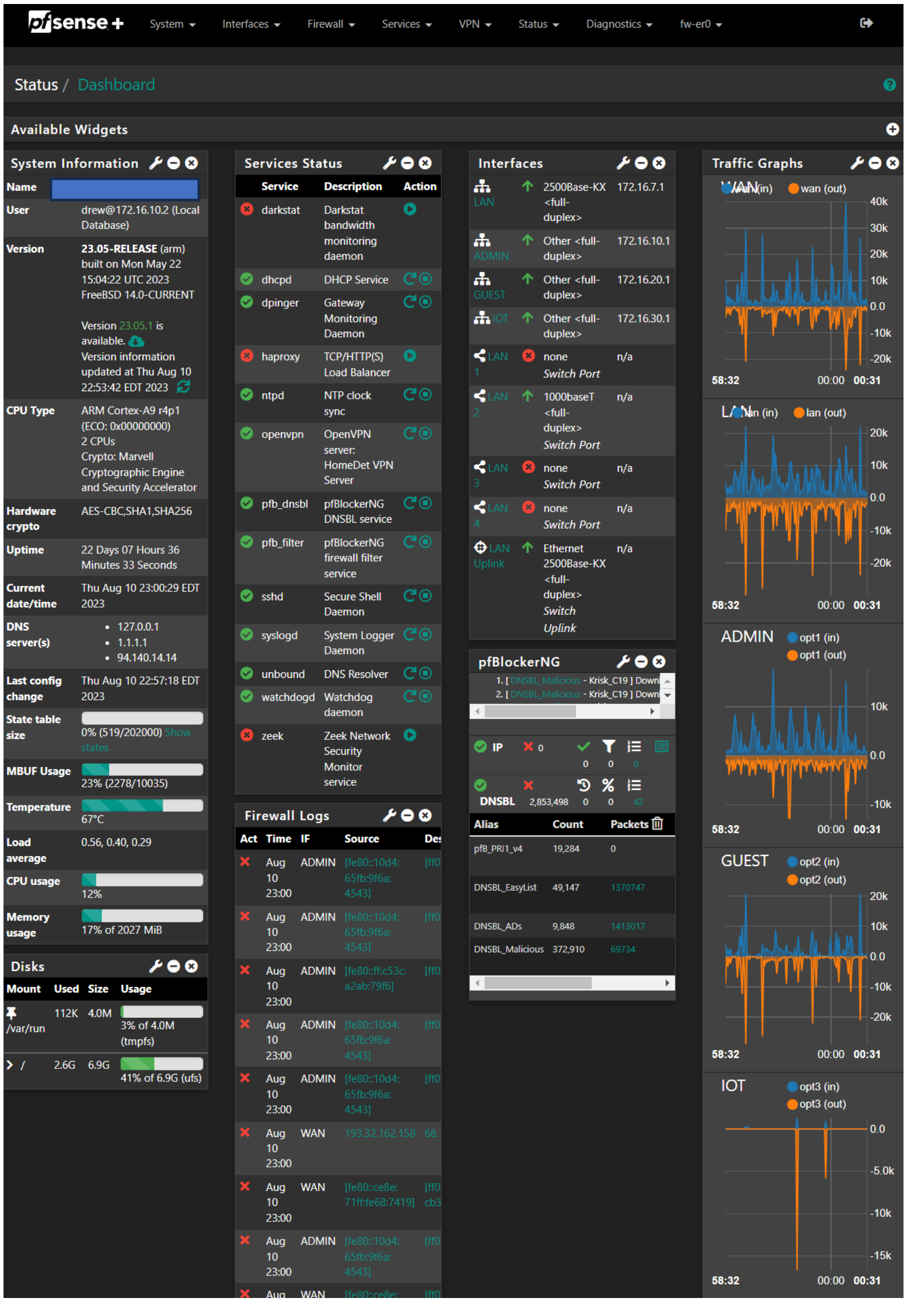
Configuration Summary:

pfsense +



Netgate pfSense Plus is developed and maintained by Netgate. © ESF 2004 - 2023 View license.

Login GUI to administer pfSense configuration profile. This login screen is not accessible beyond the local network. Firewall rules exist that protect this landing page from the outside exploits or login attempts. There are ways of accessing my local network with Virtual Private Network credentials, but this concept is beyond the scope of this paper topic.



System Information

Name	[redacted]
User	drew@172.16.10.2 (Local Database)
Version	**23.05-RELEASE** (arm) built on Mon May 22 15:04:22 UTC 2023 FreeBSD 14.0-CURRENT Version 23.05.1 is available. Version information updated at Thu Aug 10 22:53:42 EDT 2023
CPU Type	ARM Cortex-A9 r4p1 (ECO: 0x00000000) 2 CPUs Crypto: Marvell Cryptographic Engine and Security Accelerator
Hardware crypto	AES-CBC,SHA1,SHA256
Uptime	22 Days 07 Hours 36 Minutes 33 Seconds
Current date/time	Thu Aug 10 23:00:29 EDT 2023
DNS server(s)	• 127.0.0.1 • 1.1.1.1 • 94.140.14.14
Last config change	Thu Aug 10 22:57:18 EDT 2023
State table size	0% (519/202000) Show states
MBUF Usage	23% (2278/10035)
Temperature	67°C
Load average	0.56, 0.40, 0.29
CPU usage	12%
Memory usage	17% of 2027 MiB

Disks

Mount	Used	Size	Usage
/var/run	112K	4.0M	3% of 4.0M (tmpfs)
> /	2.6G	6.9G	41% of 6.9G (ufs)

Services Status

	Service	Description	Action
✗	darkstat	Darkstat bandwidth monitoring daemon	▶
✓	dhcpd	DHCP Service	
✓	dpinger	Gateway Monitoring Daemon	
✗	haproxy	TCP/HTTP(S) Load Balancer	▶
✓	ntpd	NTP clock sync	
✓	openvpn	OpenVPN server: HomeDet VPN Server	
✓	pfb_dnsbl	pfBlockerNG DNSBL service	
✓	pfb_filter	pfBlockerNG firewall filter service	
✓	sshd	Secure Shell Daemon	
✓	syslogd	System Logger Daemon	
✓	unbound	DNS Resolver	
✓	watchdogd	Watchdog daemon	
✗	zeek	Zeek Network Security Monitor service	▶

Firewall Logs

Act	Time	IF	Source	Des
✗	Aug 10 23:00	ADMIN	[fe80::10d4:65fb:9f6a:4543]	[ff0
✗	Aug 10 23:00	ADMIN	[fe80::10d4:65fb:9f6a:4543]	[ff0
✗	Aug 10 23:00	ADMIN	[fe80::ff:c53c:a2ab:79f6]	[ff0
✗	Aug 10 23:00	ADMIN	[fe80::10d4:65fb:9f6a:4543]	[ff0
✗	Aug 10 23:00	ADMIN	[fe80::10d4:65fb:9f6a:4543]	[ff0
✗	Aug 10 23:00	WAN	193.32.162.158	68.
✗	Aug 10 23:00	WAN	[fe80::ce8e:71ff:fe68:7419]	[ff0 cb3
✗	Aug 10 23:00	ADMIN	[fe80::10d4:65fb:9f6a:4543]	[ff0
✗	Aug	WAN	[fe80::ce8e:	[ff0

Interfaces

LAN	↑	2500Base-KX <full-duplex>	172.16.7.1
ADMIN	↑	Other <full-duplex>	172.16.10.1
GUEST	↑	Other <full-duplex>	172.16.20.1
IOT	↑	Other <full-duplex>	172.16.30.1
LAN 1	✗	none *Switch Port*	n/a
LAN 2	↑	1000baseT <full-duplex> *Switch Port*	n/a
LAN 3	✗	none *Switch Port*	n/a
LAN 4	✗	none *Switch Port*	n/a
LAN Uplink	↑	Ethernet 2500Base-KX <full-duplex> *Switch Uplink*	n/a

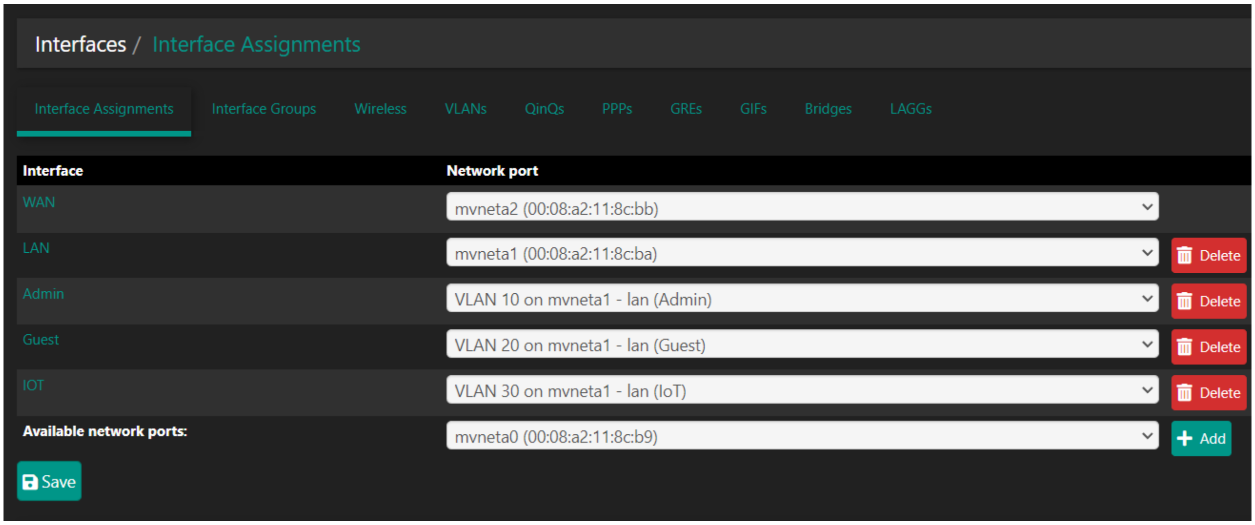
pfBlockerNG

1. [DNSBL_Malicious - Krisk_C19] Down
2. [DNSBL_Malicious - Krisk_C19] Down

✓ IP	✗ 0	✓ 0	0	0	
✓ DNSBL	✗ 2,853,498	0	% 0	42	

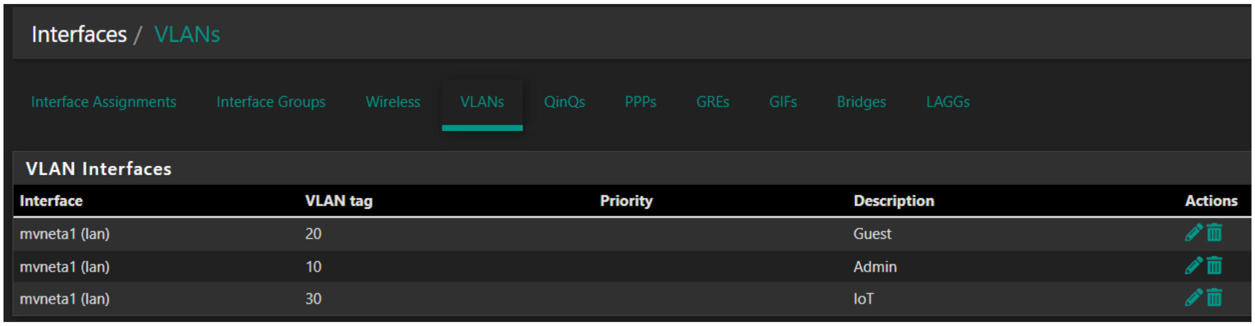
Alias	Count	Packets
pfB_PRI1_v4	19,284	0
DNSBL_EasyList	49,147	1370747
DNSBL_ADs	9,848	1413017
DNSBL_Malicious	372,910	69734

VLAN configurations began within pfSense' web-based GUI. The WAN interface is hidden for security reasons. The LAN interface profile is the primary subnet defined at 172.16.7.1. The additional subnet definitions occur in series on logical subnets: Admin (172.16.10.1), Guest (172.16.20.1), IoT (172.16.30.1). These logical subnets are the Virtual Local Area Networks and provide an extra layer of security for network segmentations as recommended in NISTs Cybersecurity Framework at the Data Security (Protect) subcategories **PR.DS-5:** Protections against data leaks (Data Security). and **PR.AC-5:** Network integrity is protected (e.g., network segregation, network segmentation) (Access Control).



Interface	Network port
WAN	mvneta2 (00:08:a2:11:8c:bb)
LAN	mvneta1 (00:08:a2:11:8c:ba)
Admin	VLAN 10 on mvneta1 - lan (Admin)
Guest	VLAN 20 on mvneta1 - lan (Guest)
IOT	VLAN 30 on mvneta1 - lan (IoT)
Available network ports:	mvneta0 (00:08:a2:11:8c:b9)

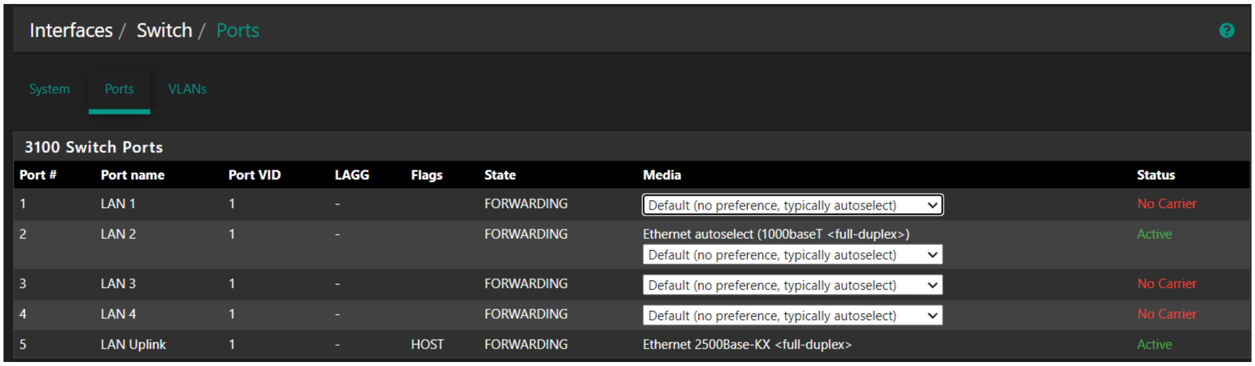
First interface assignments are given for each VLAN which is a logical segmentation of a single physical port on the Netgate firewall device.



VLAN Interfaces

Interface	VLAN tag	Priority	Description	Actions
mvneta1 (lan)	20		Guest	
mvneta1 (lan)	10		Admin	
mvneta1 (lan)	30		IoT	

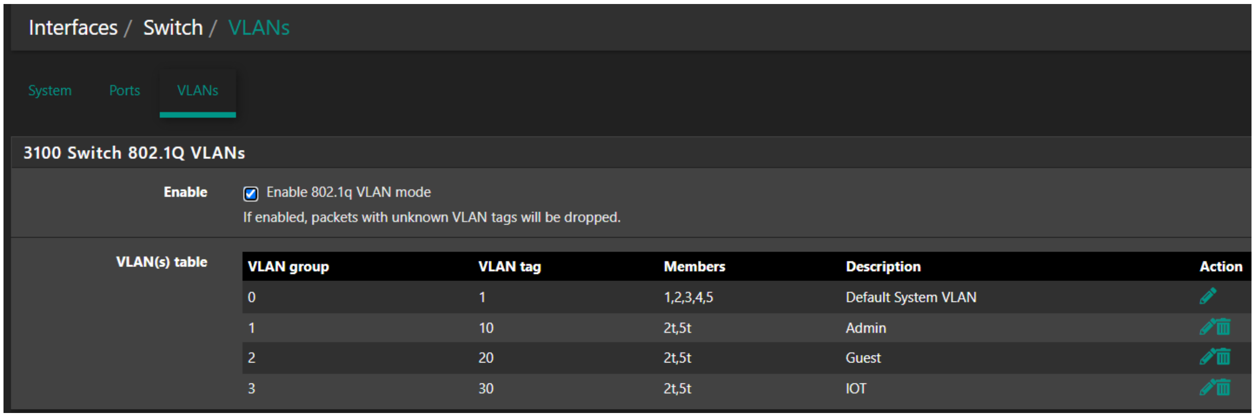
VLAN tags are defined and named accordingly Admin (10), Guest (20), IoT(30).



3100 Switch Ports

Port #	Port name	Port VID	LAGG	Flags	State	Media	Status
1	LAN 1	1	-		FORWARDING	Default (no preference, typically autoselect)	No Carrier
2	LAN 2	1	-		FORWARDING	Ethernet autoselect (1000baseT <full-duplex>) Default (no preference, typically autoselect)	Active
3	LAN 3	1	-		FORWARDING	Default (no preference, typically autoselect)	No Carrier
4	LAN 4	1	-		FORWARDING	Default (no preference, typically autoselect)	No Carrier
5	LAN Uplink	1	-	HOST	FORWARDING	Ethernet 2500Base-KX <full-duplex>	Active

Next, comes the switch assignments which identifies which ports in the firewall appliance switch are receiving and forwarding traffic and to which VLAN assignment. We must identify the ports which are active and assign Ports 2, and 5, to our newly segmented VLAN configuration profile.



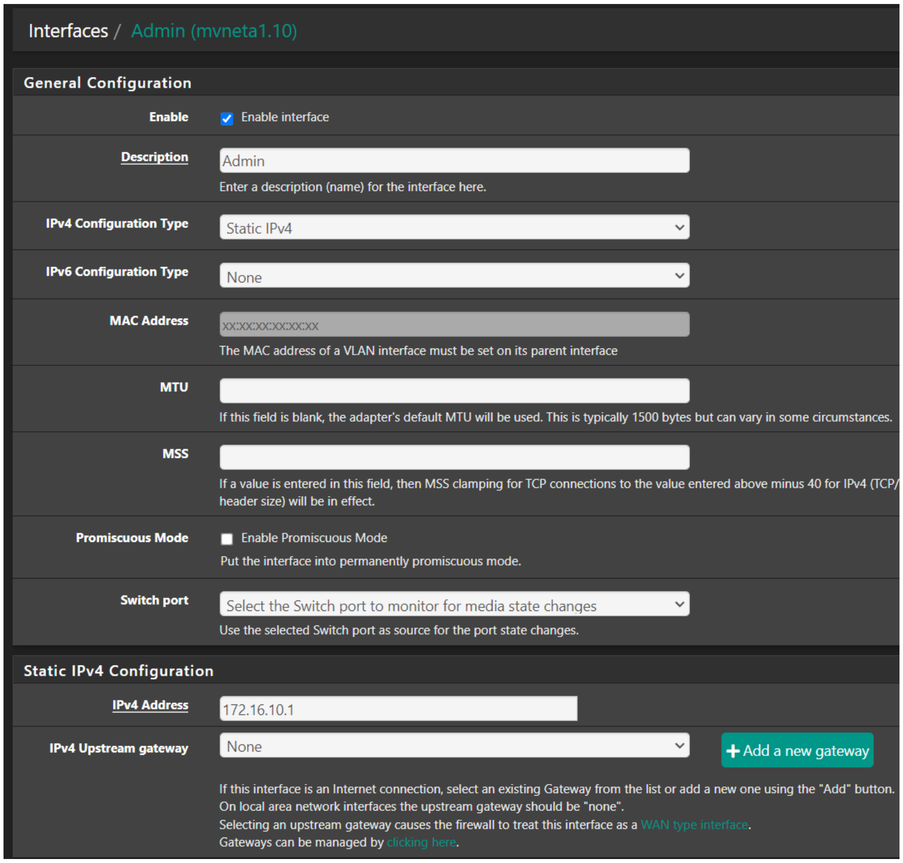
3100 Switch 802.1Q VLANs

Enable ☑ Enable 802.1q VLAN mode
If enabled, packets with unknown VLAN tags will be dropped.

VLAN(s) table

VLAN group	VLAN tag	Members	Description	Action
0	1	1,2,3,4,5	Default System VLAN	✎
1	10	2t,5t	Admin	✎🗑
2	20	2t,5t	Guest	✎🗑
3	30	2t,5t	IOT	✎🗑

Notice that we have enabled 802.1q VLAN mode. Enabling this mode introduces the ethernet frame VLAN ID. Our local network is now prepared to read these VLAN ID's and properly forward their traffic to their respective VLAN groups. Also take not of the Members column for VLAN groups, 1,2,3. These groups where assigned their VLAN tag IDs and also provided their physical switch assignments located at Ports 2, and 5.



General Configuration

Enable ☑ Enable interface

Description Admin
Enter a description (name) for the interface here.

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address xx:xx:xx:xx:xx:xx
The MAC address of a VLAN interface must be set on its parent interface

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/ header size) will be in effect.

Promiscuous Mode ☐ Enable Promiscuous Mode
Put the interface into permanently promiscuous mode.

Switch port Select the Switch port to monitor for media state changes
Use the selected Switch port as source for the port state changes.

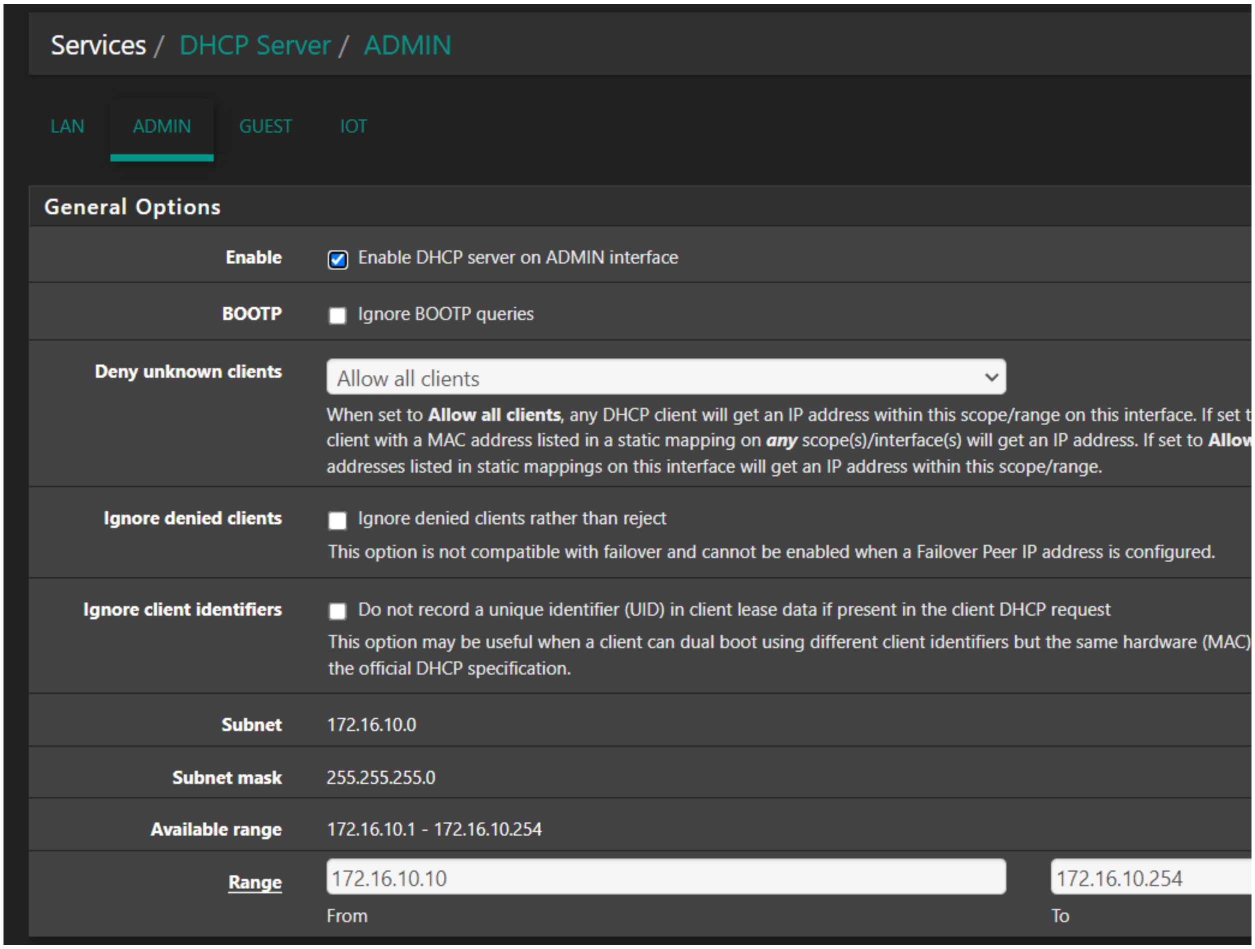
Static IPv4 Configuration

IPv4 Address 172.16.10.1

IPv4 Upstream gateway None

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by clicking here.

Following these configurations, we now must enable each of the Admin (172.16.10.1), Guest (172.16.20.1), and IoT (172.16.30.1) interfaces and assign their static IPv4 addresses. This establishes each respective subnet (/24) and prepares FOR further configurations.



Services / DHCP Server / ADMIN

General Options

Enable ☑ Enable DHCP server on ADMIN interface

BOOTP □ Ignore BOOTP queries

Deny unknown clients Allow all clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set t client with a MAC address listed in a static mapping on ***any*** scope(s)/interface(s) will get an IP address. If set to **Allow** addresses listed in static mappings on this interface will get an IP address within this scope/range.

Ignore denied clients □ Ignore denied clients rather than reject

This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers □ Do not record a unique identifier (UID) in client lease data if present in the client DHCP request

This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) the official DHCP specification.

Subnet 172.16.10.0

Subnet mask 255.255.255.0

Available range 172.16.10.1 - 172.16.10.254

Range 172.16.10.10 From 172.16.10.254 To

We also want to ensure that we enable DHCP servers on each of our VLANs. This ensures IP addressing without the need for manually addressing. This is pretty much all the necessary configuration needed within pfSense. These assignments will not segment a network alone and requires further configurations with a managed switch. Additionally, this is only enabling physical ethernet Internet access. Wi-Fi access requires its own configuration later on.

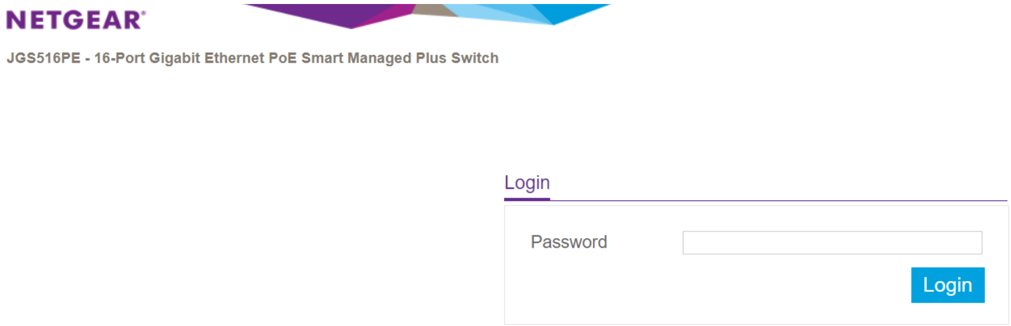
b. Netgear JGS516PE 16-Port 8-POE Gigabit Ethernet Managed Switch

JGS516PE — 16-Port Gigabit Ethernet Plus Switch with 8 Ports PoE

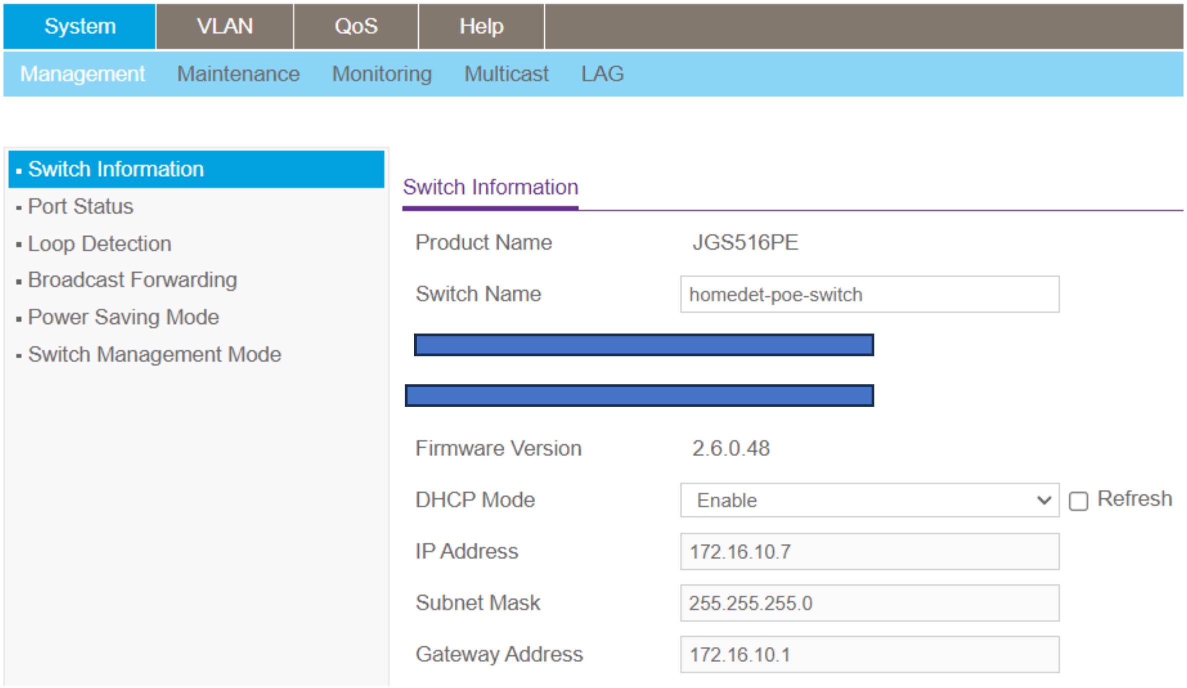
Category	Description
Gigabit Ports	16
# POE Ports	8
Total POE Watts	85 Watts
Bandwidth	32Gbps
Priority Queuing	Weighted Round Robin (WRR)
Jumbo Frame	Up to 9k packet size
L2 Services – VLAN VLAN(#Supported)	100
IEEE 802.1Q VLAN Tagging	Yes
Port-Based VLAN	Yes
L3 Services – DHCP	Yes
IEEE Network Protocols	• IEEE 802.3 Ethernet • IEEE 802.3i 10BASE-T • IEEE 802.3u 100BASE-T • IEEE 802.3ab 1000BASE-T • IEEE 802.1p Class of Service • IEEE 802.3af (PoE) • IEEE 802.1Q VLAN Tagging • IEEE 802.3x Full-duplex Flow Control
Cooling	Active (fan)
Power	External ITE P/S AC/DC 100-240V, 50-60 Hz, 12V 3.33A, threaded barrel connector AC Inlet: IEC320-C14 (3 PIN) One US, UK, EU or ANZ power cord included US Power Cord: NEMA 5-15P to IEC320-C13 UK Power Cord: BS 1363 to IEC320-C13

Category	Description
	EU Power Cord: CEE7/16 to IEC320-C13 ANZ Power Cord: AS 3112 to IEC320-C13
Environmental	32°F (0°C) to 149°F (65°C)
Certifications	FCC, CE, RoHS, UL, IEC-60950

Configuration Summary:


NETGEAR
JGS516PE - 16-Port Gigabit Ethernet PoE Smart Managed Plus Switch
Login
Password
Login

Login GUI for the managed POE switch. Management login enables further VLAN configuration needed to continue network segmentation.



Product Name JGS516PE

Switch Name homedet-poe-switch

[redacted]

[redacted]

Firmware Version 2.6.0.48

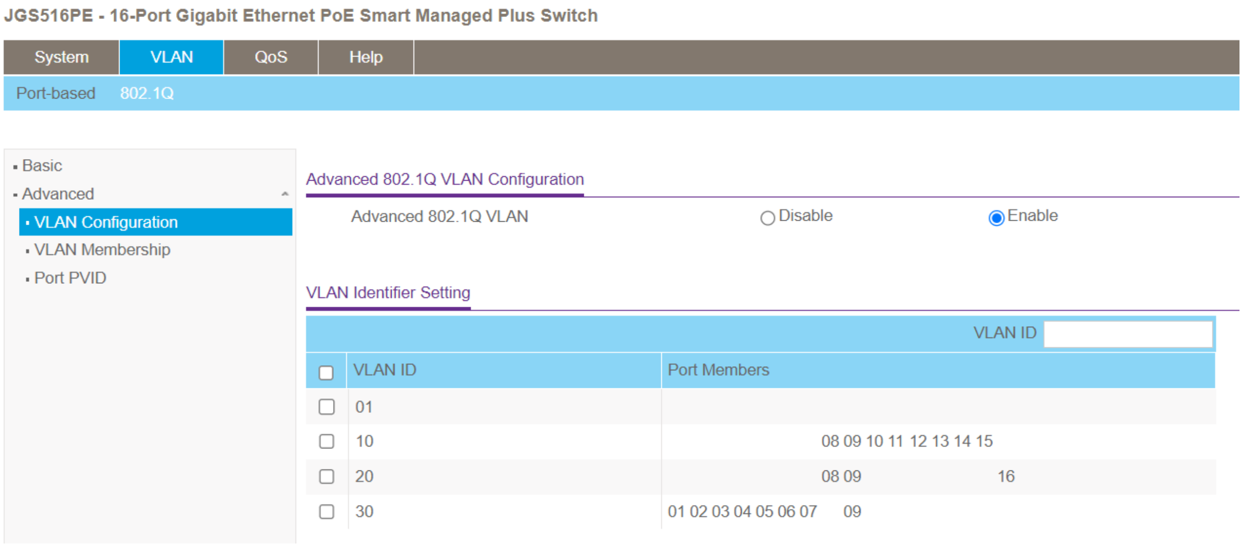
DHCP Mode Enable □ Refresh

IP Address 172.16.10.7

Subnet Mask 255.255.255.0

Gateway Address 172.16.10.1

Once logged in, review system specifications. Note the IP address subnet assignment to our Admin (172.16.10.7). This was statically assigned previously.



Advanced 802.1Q VLAN Configuration

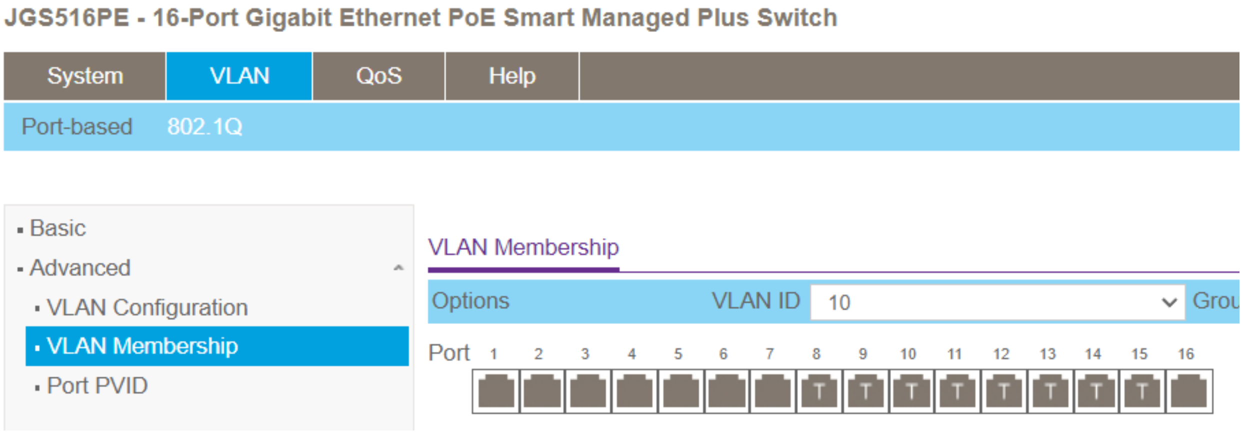
Advanced 802.1Q VLAN ○ Disable ● Enable

VLAN Identifier Setting

VLAN ID

□	VLAN ID	Port Members
□	01	
□	10	08 09 10 11 12 13 14 15
□	20	08 09 16
□	30	01 02 03 04 05 06 07 09

Since the VLAN ID's have already been established in a previous step on the pfSense firewall software, in the managed switch we need to define which of the 16 ports will be reserved for which VLAN ID. For traffic to be routed properly, a single port which is Port 9, must be "Trunked" across all three VLAN ID's. This is the main vein of incoming and outgoing data frames which will be routed based on the ethernet frame VLAN ID and the accompanying IP address assignment.

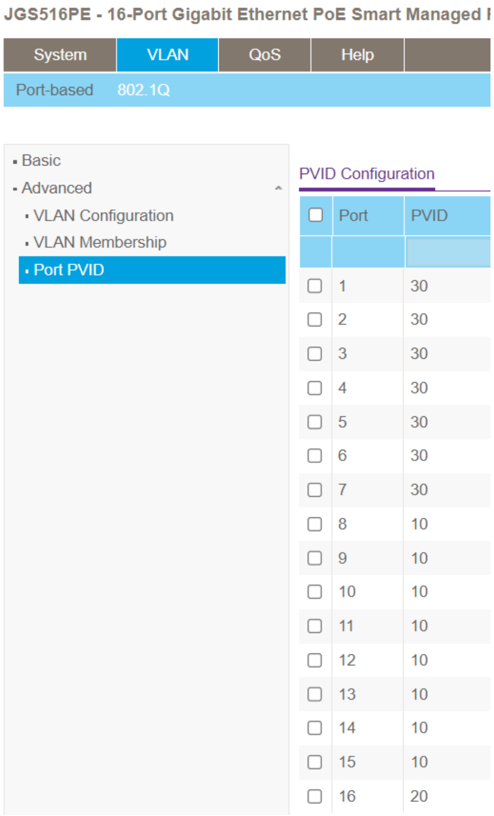


VLAN Membership

VLAN ID 10

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
								T	T	T	T	T	T	T	T	

This is the VLAN membership configuration page that assigns which ports belong to which VLAN ID. Notice the VLAN ID drop down box selected to 10; this means any device that is hard wired into ports 8-15 will be assigned to Admin subnet (172.16.10.1-.255) and their Tagged ("T") traffic will deliver only to these 8-ports reserved for Admin devices.



PVID Configuration

□	Port	PVID
□	1	30
□	2	30
□	3	30
□	4	30
□	5	30
□	6	30
□	7	30
□	8	10
□	9	10
□	10	10
□	11	10
□	12	10
□	13	10
□	14	10
□	15	10
□	16	20

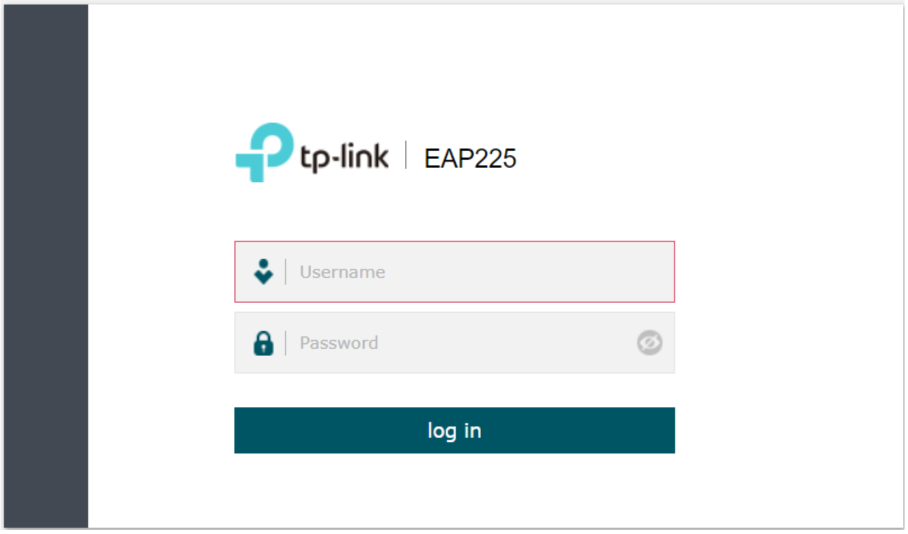
This page is the explicit definition for assigning the switch ports to a respective VLAN ID. Where the configurations above define how the traffic segments and routes across or around one or more VLANs. IT can become cumbersome and a bit confusing, but it becomes clearer once students can engage with the configuration and management process.

c. TP-Link EAP225 Wi-Fi Access Point

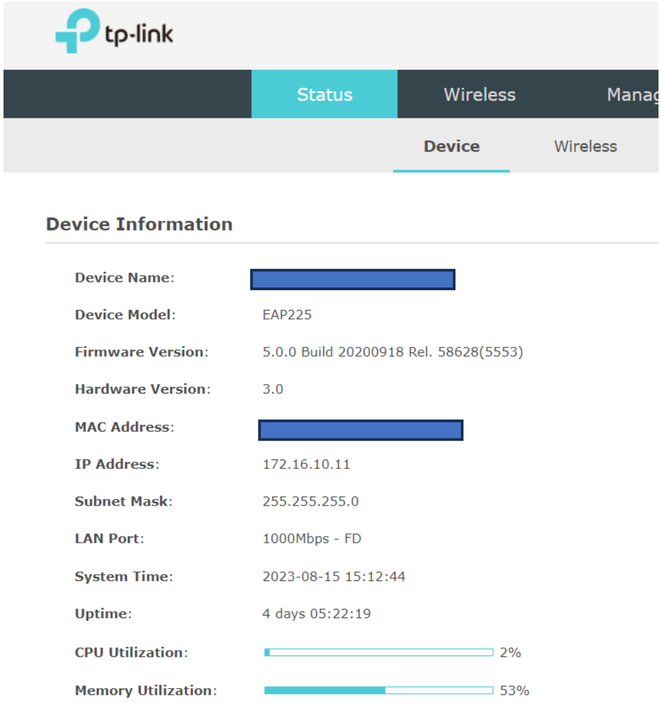
AC1350 Wireless MU-MIMO Gigabit Ceiling Mount Access Point

Category	Description
Interface	Gigabit Ethernet (RJ-45) Portx1 (Support IEEE802.3af PoE and Passive PoE
Physical Security Lock	Yes
Power Supply	802.3af/at PoE 24v Passive PoE (+4.5pins; -7.8 pins, PoE Adapter Included)
Power Consumption	US: 12.6 W
Dimensions	8.1 x 7.1 x 1.5 in
Antenna Type, Frequencies and Signal Rates	3 Internal Omni 2.4 GHz: 4 dBi: Up to 450 Mbps 5 GHz: 5 dBi: Up to 867 Mbps
Wireless Standards	IEEE 802.11ac/n/g/b/a
SSH and Web-based Management	Yes – HTTP, HTTPS
Management VLAN	Yes

Configuration Summary:



This is the login screen for the wireless access point which enables wireless internet access across the network.



Device Information

Device Name: [redacted]

Device Model: EAP225

Firmware Version: 5.0.0 Build 20200918 Rel. 58628(5553)

Hardware Version: 3.0

MAC Address: [redacted]

IP Address: 172.16.10.11

Subnet Mask: 255.255.255.0

LAN Port: 1000Mbps - FD

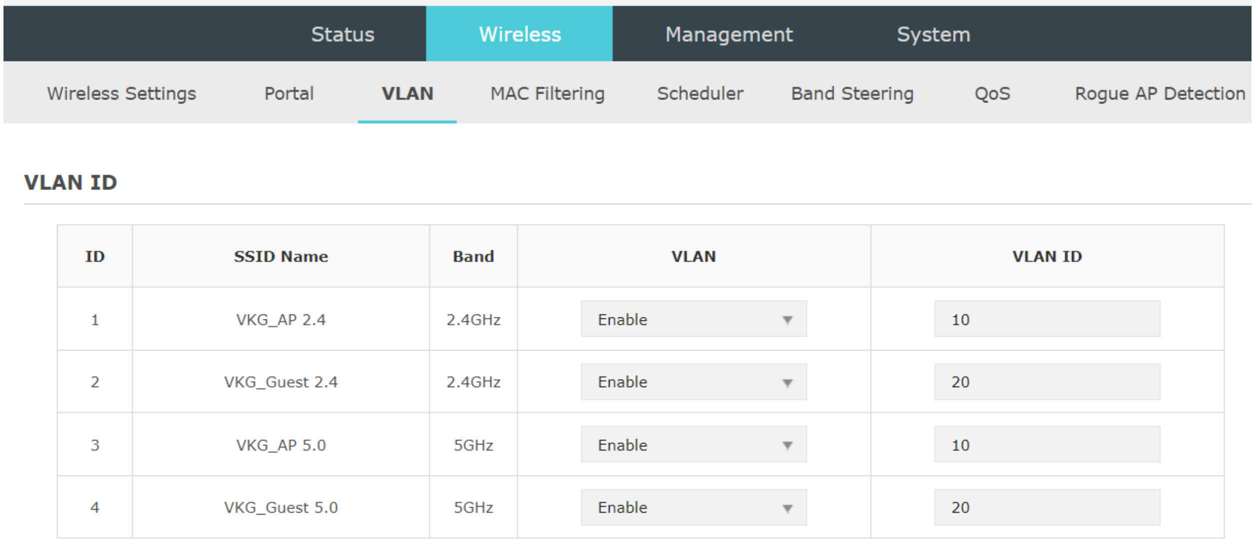
System Time: 2023-08-15 15:12:44

Uptime: 4 days 05:22:19

CPU Utilization: 2%

Memory Utilization: 53%

Initial login directs and automatically assigns an IP for this Power-Over-Ethernet (POE) wireless access point (WAP) via DHCP. Based on our configurations, this device can receive an DHCP assignment from four LANs depending on where we connect our WAP ethernet cable. It is important to decide whether one, two, or three VLANs require wireless Internet access. Depending on what devices are connected to the Admin VLAN may require cellphone access to a server database, whether it is connected to subnet .20 or .10. To achieve these connections across these two VLANs we must ensure Port 8 is configured for both VLAN ID 10 and 20 in our managed switch configuration in the last section. This port must also be configured for Tagged traffic to properly segregate data transmissions. An Untagged ("U") definition of Port 8 will deliver all transmitted traffic to end hosts connected through Port 8. This means all devices connected to the WAP will have the ability to read all packets and their destinations should an end host decide to "sniff" network traffic. This aspect of tagged vs. untagged is crucial to maintaining VLAN traffic segregation via their respective VLAN ID frames.



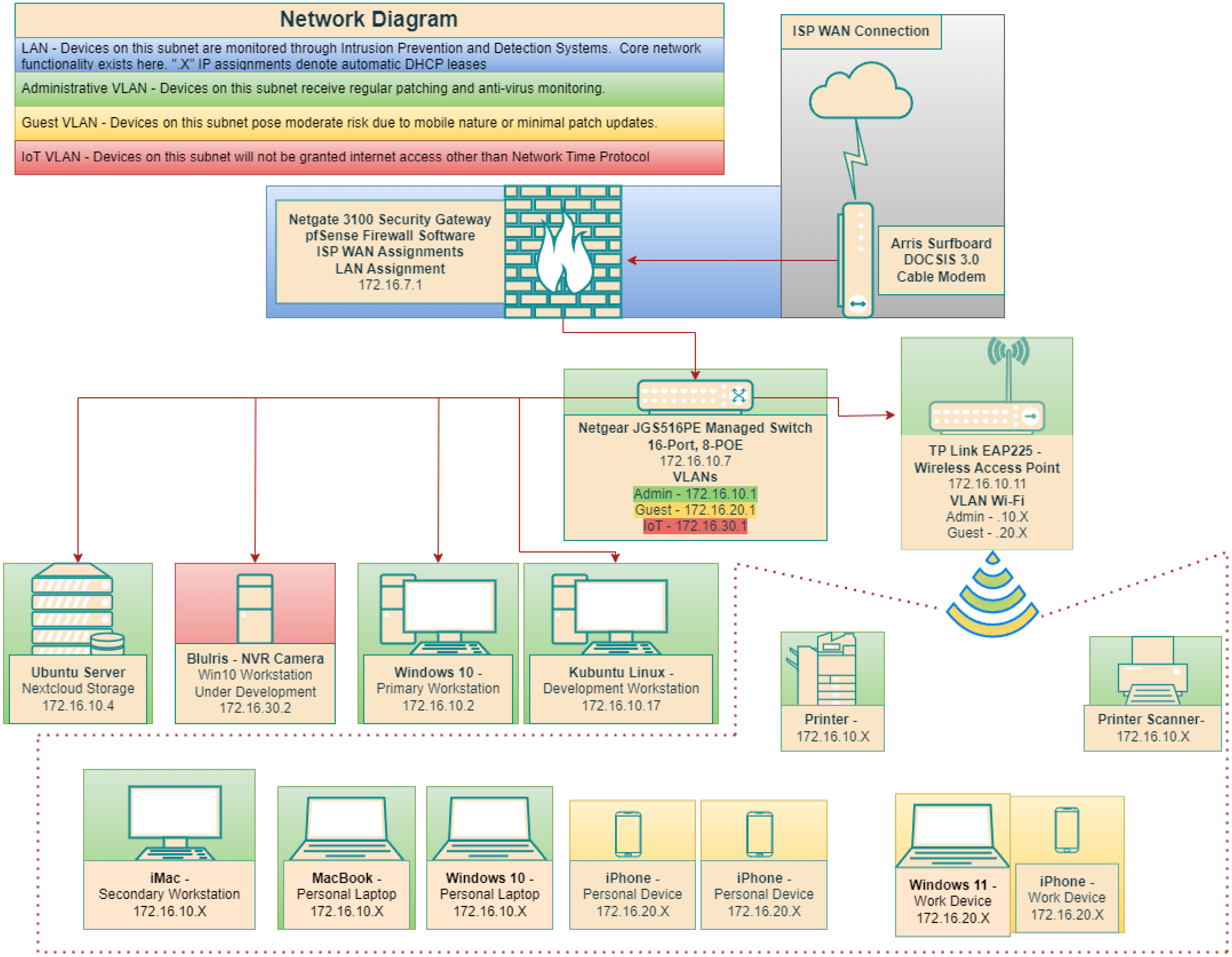
VLAN ID

ID	SSID Name	Band	VLAN	VLAN ID
1	VKG_AP 2.4	2.4GHz	Enable	10
2	VKG_Guest 2.4	2.4GHz	Enable	20
3	VKG_AP 5.0	5GHz	Enable	10
4	VKG_Guest 5.0	5GHz	Enable	20

The configuration page for the WAP allows for our VLAN configurations. Here are four Service Set Identifier (SSID) being broadcasted from one access point. Both the Admin (.10) and Guest (.20) VLANs can transmit traffic via 2.4GHz and 5GHz frequencies.

VI. Overall Network Configuration Summary

Typical home network models happen by chance in the order in which devices are added to networks with absent or minimal forethought so long as Internet Service Provider (ISP) IP addressing occurs at the ISP provided modem across a pre-configured private network subnet. There are three private subnet reservations established by Internet Corporation for Assigned Names and Numbers (ICANN) in the ranges, 192.168.0.0 to 192.168.255.255, 172.16.0.0 to 172.31.255.255, and finally 10.0.0.0 to 10.255.255.255. Each of these ranges are referred to as Class C, Class B, and Class A respectively. There is a subnet mask associated with each of these ranges 255.255.0.0 or /16 for Class C, 255.240.0.0 or /12 for Class B, and 255.0.0.0 or /8 for Class A. Class A networks are typically used in large organizations, Class B networks are typically used in medium-sized organizations and Class C are typically for smaller networks such as home or small-businesses. For our demonstration purposes LAN assignment occurred within the 172.16.0.0 – 172.31.255.255 with a subnet of /24.



Network Diagram

LAN - Devices on this subnet are monitored through Intrusion Prevention and Detection Systems. Core network functionality exists here. ".X" IP assignments denote automatic DHCP leases

Administrative VLAN - Devices on this subnet receive regular patching and anti-virus monitoring.

Guest VLAN - Devices on this subnet pose moderate risk due to mobile nature or minimal patch updates.

IoT VLAN - Devices on this subnet will not be granted internet access other than Network Time Protocol

ISP WAN Connection

Arris Surfboard
DOCSIS 3.0
Cable Modem

Netgate 3100 Security Gateway
pfSense Firewall Software
ISP WAN Assignments
LAN Assignment
172.16.7.1

Netgear JGS516PE Managed Switch
16-Port, 8-POE
172.16.10.7
VLANs
Admin - 172.16.10.1
Guest - 172.16.20.1
IoT - 172.16.30.1

TP Link EAP225 -
Wireless Access Point
172.16.10.11
VLAN Wi-Fi
Admin - .10.X
Guest - .20.X

Ubuntu Server
Nextcloud Storage
172.16.10.4

BluIris - NVR Camera
Win10 Workstation
Under Development
172.16.30.2

Windows 10 -
Primary Workstation
172.16.10.2

Kubuntu Linux -
Development Workstation
172.16.10.17

Printer -
172.16.10.X

Printer Scanner-
172.16.10.X

iMac -
Secondary Workstation
172.16.10.X

MacBook -
Personal Laptop
172.16.10.X

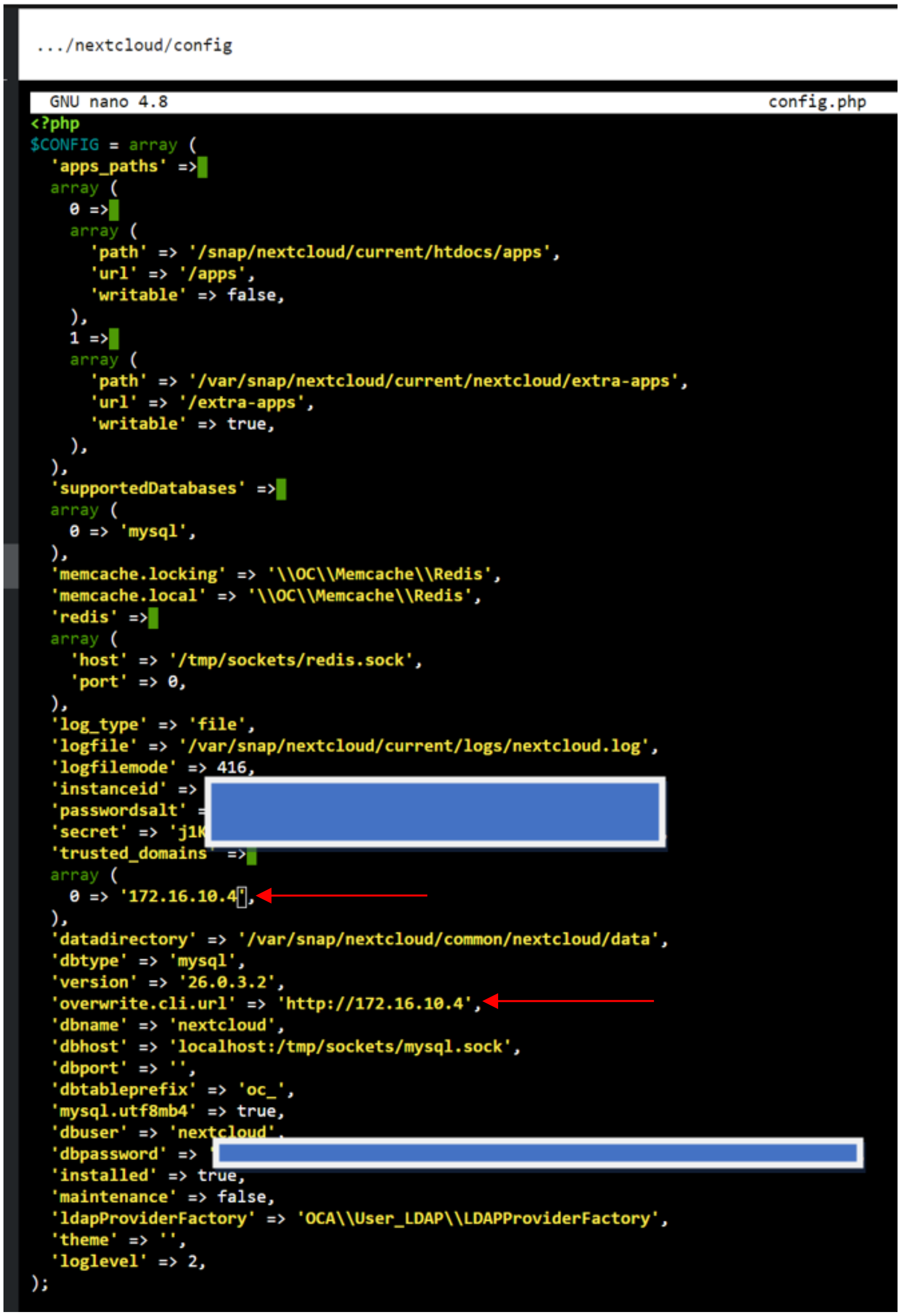
Windows 10 -
Personal Laptop
172.16.10.X

iPhone -
Personal Device
172.16.20.X

iPhone -
Personal Device
172.16.20.X

Windows 11 -
Work Device
172.16.20.X

iPhone -
Work Device
172.16.20.X



```
.../nextcloud/config

  GNU nano 4.8                                                      config.php
<?php
$CONFIG = array (
  'apps_paths' =>
  array (
    0 =>
    array (
      'path' => '/snap/nextcloud/current/htdocs/apps',
      'url' => '/apps',
      'writable' => false,
    ),
    1 =>
    array (
      'path' => '/var/snap/nextcloud/current/nextcloud/extra-apps',
      'url' => '/extra-apps',
      'writable' => true,
    ),
  ),
  'supportedDatabases' =>
  array (
    0 => 'mysql',
  ),
  'memcache.locking' => '\\OC\\Memcache\\Redis',
  'memcache.local' => '\\OC\\Memcache\\Redis',
  'redis' =>
  array (
    'host' => '/tmp/sockets/redis.sock',
    'port' => 0,
  ),
  'log_type' => 'file',
  'logfile' => '/var/snap/nextcloud/current/logs/nextcloud.log',
  'logfilemode' => 416,
  'instanceid' => [redacted]
  'passwordsalt' =
  'secret' =>
  'trusted_domains' =>
  array (
    0 => '172.16.10.4',
  ),
  'datadirectory' => '/var/snap/nextcloud/common/nextcloud/data',
  'dbtype' => 'mysql',
  'version' => '26.0.3.2',
  'overwrite.cli.url' => 'http://172.16.10.4',
  'dbname' => 'nextcloud',
  'dbhost' => 'localhost:/tmp/sockets/mysql.sock',
  'dbport' => '',
  'dbtableprefix' => 'oc_',
  'mysql.utf8mb4' => true,
  'dbuser' => 'nextcloud',
  'dbpassword' => [redacted]
  'installed' => true,
  'maintenance' => false,
  'ldapProviderFactory' => 'OCA\\User_LDAP\\LDAPProviderFactory',
  'theme' => '',
  'loglevel' => 2,
);
```

This screenshot is a configuration file for a local storage database on my home network. Since this database network connection was reconfigured for a new subnet assignment, previous static IP addressing prevented the Dynamic Host Configuration Protocol (DHCP) addressing request for a new IP address. This means manual addressing updates were needed within service configuration files to allow addressing on new network parameters. In my previous configurations, 172.16.7.7 was statically assigned to the storage server which required updating to 172.16.10.4. The .10 subnet is a new administrative VLAN definition within the pfSense firewall software.

References

1) National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0, National Institute of Standards and Technology, 12 Feb. 2014, https://www.nist.gov/document/cybersecurity-framework-021214pdf.
2) National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. NIST Cybersecurity Framework Version 1.1, National Institute of Standards and Technology, 16 Apr. 2018, https://doi.org/10.6028/NIST.CSWP.04162018.
3) National Institute of Standards and Technology. "Security and Privacy Controls for Information Systems and Organizations." NIST Special Publication 800-53 Revision 5, U.S. Department of Commerce, September 2020, https://doi.org/10.6028/NIST.SP.800-53r5.
4) National Institute of Standards and Technology. https://www.nist.gov/cyberframework/getting-started/quick-start-guide
5) National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 2.0, National Institute of Standards and Technology, 08 Aug. 2023, https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20
6) University of Aberdeen, https://erg.abdn.ac.uk/users/gorry/course/lan-pages/vlan.html - Accessed 08 Aug2023, Down 15August2023. I think this server was accidentally indexed and since patched to disallow access.
7) https://docs.netgate.com/pfsense/en/latest/solutions/sg-3100/index.html
8) https://docs.netgate.com/pfsense/en/latest/solutions/sg-3100/hardware-specs.html
9) https://docs.netgate.com/pfsense/en/latest/network/subnets.html?highlight=subnet
10) https://docs.netgate.com/pfsense/en/latest/network/cidr.html
11) https://www.netgear.com/support/product/jgs516pe#docs
12) https://www.tp-link.com/us/business-networking/omada-sdn-access-point/eap225/v3/#specifications
13) SANS Institute, *Critical Security Controls*, www.sans.org/critical-security-controls/
14) ISACA, *Transforming Cybersecurity: Using COBIT 5*, 2013