Personal VLAN

CS455, Professor Akbarfam
Rahul Parulkar: Rahul.parulkar@wsu.edu
Ethan Kanyid: ethan.kanyid@wsu.edu
Peter Lagonegro: peter.lagonegro@wsu.edu
Jonahtan Vasquez: jonahtan.vasquez@wsu.edu

ABSTRACT. This project is directed at setting up a virtual local area network (VLAN) on a standard home router to test how network segmentation can improve security and organization. An unmodified NETGEAR R6900P running with OEM firmware can be configured to operate several VLANs through the router's advanced settings. Additionally, there are also custom firmware's that can be flashed onto the router, and although these provide more customizability, they also force more complexity. Each VLAN can be altered to have its own ID, subnet, and ports - which is useful for separating network traffic for different types of devices. These VLANs range in purpose, but common VLANs include a home network, guest network, and Internet of Things (IoT) network. Moreover, some devices include personal computers (PCs), cameras, mobile phones, or even smart fridges. Through this project, it will be demonstrated how VLAN's are useful for network segmentation and organization, so that your fridge cannot communicate with your PC.

I. INTRODUCTION

VLANs are used to separate network traffic without needing extra hardware – essentially, they work alongside a regular local area network (LAN) to provide an additional virtual LAN. They are standard practice in enterprise, industrial cyber security environments to isolate, protect, and segment assets. Although they are common in large networks, home networks can also benefit from VLANs, even on consumer equipment. The goal is to split devices like personal computers, IoT gadgets, and guests into separate groups so they do not interfere with one another. This project will use a NETGEAR R6900P router using the router's built-in interface, without the need to install custom firmware or connect any external switches.

II. BACKGROUND

Ethernet is the foundational technology for wired networking, introduced in the 1970s and later standardized as IEEE 802.3. It enables devices to communicate over physical cables using MAC addresses for identification. Wi-Fi, or wireless LAN, became popular in the late 1990s and is defined by the IEEE 802.11 family of standards. It allows devices to connect to networks wirelessly, trading off some speed and reliability for mobility and convenience. Ethernet and Wi-Fi are two mediums for internet communication and are necessary for the development of a VLAN.

The next components of VLANs are routers and switches. A switch connects multiple devices to forward information. A router, on the other hand, connects different networks (e.g., a home network to the internet). Switches operate at Layer 2 (Data Link) of the OSI model, while routers operate at Layer 3 (Network). It is also important to note that most consumer routers are both routers and switches.

As networks grew more complex, organizations needed better ways to segment traffic without adding more physical infrastructure. This led to the development of Virtual LANs (VLANs). VLANs, formalized in the IEEE 802.1Q standard in 1998, allow a single physical network to be logically divided into multiple broadcast domains. VLANs combine these previously mentioned technologies and create virtual networks with them.

III. RELATED WORK

VLANs are typically implemented using professional equipment or open-source router firmware like DD-WRT or OpenWRT. For this project, we wanted to see how much could be done with just the stock NETGEAR firmware. NETGEAR's documentation confirms that VLAN tagging is available on this model, though it's not as flexible as enterprise systems. This made it a good candidate for testing basic segmentation in a small network.

IV. SYSTEM DESIGN / METHODOLOGY

To implement and test VLAN segmentation, we will use a NETGEAR Nighthawk – which supports VLAN configuration. The initial step would be to configure multiple VLANs on the router. An example representation of the configuration could be VLAN 10 for IoT devices, VLAN 20 for Personal PC's, and VLAN 30 for Admins or Guests. After VLAN configuration, connectivity testing will be performed to verify each segmentation. A ping test will be performed to verify isolation between different VLANs. Various other potential tests will be later performed to test performance under simulated DoS attacks, iperf3 to measure throughput and latency, Nmap could be used to test for cross-VLAN visibility. This is to ensure devices on one VLAN cannot detect or connect to devices on another VLAN. Finally, we could utilize WireShark to analyze broadcast traffic and traffic separation before and after VLAN configuration.

V. IMPLEMENTATION / EXPERIMENT SETUP

The router was configured with three VLANs, each meant for a different type of traffic:

VLAN 1 – MainNet (192.168.1.x): The default management network.
VLAN 10 – IoTNet (192.168.10.x): Set up for 2.4 GHz Wi-Fi devices.
VLAN 20 – GuestNet (192.168.20.x): Set up for 5 GHz Wi-Fi users.

The VLANs were created under Advanced → Setup → VLAN / Bridge Settings. VLAN IDs 10 and 20 were added with priority 0, and each was tied to a separate wireless band. The default VLAN 1 remained unchanged for management access. Multiple devices can then be on these different LANs to test the network segmentation.

VI. PRELIMINARY RESULTS OR PROGRESS

Three VLANs have been set up on the router, however the router crashes if not done perfectly.

VII. DISCUSSION / NEXT STEPS

The next step for this project is to ensure that we can reliably set up the VLANs without the router needing to be restarted. Simulate a DoS attack and see how the VLANs hold up. Also, we can try to mitigate the DoS attack using the built in software on the router.

VIII. CONCLUSION

VLANs can be implemented on consumer routers with a reasonable amount of effort but are seemingly unreliable compared to the equipment available to enterprises. Our current efforts to set up VLANs on a NETGEAR AC1900 router have shown us that even though it is possible to set up multiple VLANs, there have been insufficient tests to prove the efficacy and efficiency of multiple VLANs. However, with more experimentation and thorough documentation, a more comprehensive outlook can be garnered on VLANs – and most importantly a guiding document can bring inexperienced individuals to understand and implement their own VLAN.

REFERENCES

[1] Netgear, "What is a vlan?," NETGEAR KB, https://kb.netgear.com/24720/What-is-a-VLAN (accessed Oct. 7, 2025).

[2] Netgear, "What do I need to know about setting up vlans?," NETGEAR KB, https://kb.netgear.com/000048453/What-do-I-need-to-know-about-setting-up-VLANs (accessed Oct. 7, 2025).

[3] Nighthawk® AC1900 SMART WIFI Router—dual band Gigabit, https://www.netgear.com/images/datasheet/networking/wifirouter/R6900P.pdf (accessed Oct. 8, 2025).

[4] Netgear, "How do I set up a bridge for a VLAN tag group on my Nighthawk Router?," NETGEAR KB, https://kb.netgear.com/25724/VLAN-tagging-setup-for-Nighthawk-router (accessed Oct. 7, 2025).