Connor Cruz
6 January 2026
Honor Above All
Security Controls to Mitigate Vulnerabilities in a Switched LAN

Executive Summary

This assessment analyzes the security of a school's LAN. While the school LAN is operational, it is not configured for security purposes. One significant vulnerability is the lack of any VLAN segmentation on the network, which allows visibility between all devices and could potentially lead to lateral movement within the LAN to perform actions such as gaining access to administrative servers, elevating privileges, and access to private data. The network contains a lack of security and authentication, with there being no port security enabled and no authentication requirements to connect to switch ports. This vulnerability has the potential risk of allowing any unauthorized device being able to connect into, and access the network and gaining access into any device. This also includes the risk of interception of user data by allowing attackers to gain access to network traffic. A notable physical vulnerability also exists: important network devices are left in unlocked rooms during school hours, which could lead to malicious tampering with physical hardware and the risk of access to the network and security controls.

To address lateral movement across the network, VLAN segmentation can be implemented and adequately moderated through switch and router settings. Furthermore, these settings can be modified to implement DHCP snooping to allow for DAI, thus also mitigating the risk for attacks on open ports or from unauthorized devices. Regarding physical concerns, hardware and network devices should be physically secured and locked, allowing only identified personnel entry with security badges and keys used to allow access to server and network rooms with important devices.

1. System/Network Overview

The school's network is a switched LAN, with one managed switch. There are a total of eighteen endpoints on the network. The endpoints consist of the following: twelve student laptops, four teacher laptops, one administrator workstation, and one server. The network does not contain any network segmentation, as no VLANs are configured, thus making all devices visible to each other. There are also no existing security controls: there is no port security enabled and no authentication present on switch ports. There are minimal physical security controls, with server rooms remaining unlocked during school hours. This assessment will be performed over the entire network to assess vulnerabilities and potential solutions.

2. Observations & Evidence Collected

To begin the analysis, the server device's interface information was found using "ip addr", and its routing information was found via "ip route" (see **Appendix A**). This screenshot specifically displays the server device's IP configuration, as well as its routing table. The host is assigned an IP address of 10.12.18.128/20, with the subnet mask allowing for a large range of IP addresses. The routing table also displays a single route for the server device's subnet and a default gateway within the same subnet. The absence of any routed VLANs and the existence of only necessary interfaces suggests that devices within the network are grouped together. This network structure increases device exposure, as any host within the network can interact directly with others with minimal limits in communication.

Connected devices on the network are able to directly discover and communicate with one another. When the 'arping' utility was used on a student host device to send ARP requests to the server host on the LAN over the enp0s1 interface, all five ARP requests received replies with the MAC address of the server device, a2:60:90:be:1f:00 (see **Appendix B**). The lack of packet loss demonstrates that ARP resolution occurs on the network without any restriction. Since ARP is only able to operate in its respective broadcast domain, the student and server devices must reside within the same subnet without any separation via VLANs or access lists. Uninterrupted communication applies to any two devices on the network, implying that all devices can directly interact with each other.

ARP broadcast was also found to be visible across multiple devices. Capturing live ARP traffic through the server device received requests for multiple host names, notably MaryBuwicksAir, JTStreamingMBP, and _gateway (see **Appendix C**). The server device is assigned a hostname of MaryBuwicksAir, so the screenshot displays ARP requests for any hostname and replies to requests for its hostname. All ARP traffic is visible without any filtering or restriction, suggesting that broadcast information is shared among all devices in the network. The unfiltered presence of these ARP requests indicates a lack of dynamic ARP inspection, as well as any VLAN segmentation.

3. Identified Vulnerabilities (minimum 6)

Vulnerability 1: Flat Network Architecture

The network consists of a flat broadcast domain with no VLAN segmentation to separate student, teacher, administrator, or server devices. In a school setting, a flat network architecture allows all devices to directly communicate with and observe important devices, such as an administrator workstation and server. This unlimited access increases the risk of unauthorized access to sensitive information, such as grades, administrative decisions, and student information.

Vulnerability 2: Lack of Switch Port Security

The managed switch does not enforce any port security controls, such as assigning specific devices to certain ports and limiting the amount of MAC addresses which can be assigned to a port. This lack of port security allows any device to be physically connected to a switch port to gain complete network access. Since devices are frequently moved by both students and faculty in a school, unauthorized devices could both unintentionally and intentionally be connected to the LAN, allocating network resources to unintended devices or allowing malicious activity from inside of the network.

Vulnerability 3: Non-Restricted DHCP Services

The network never specifies which devices are permitted to host DHCP services, thus allowing any device in the network to act as a DHCP server. With a school setting featuring many important devices, rogue DHCP servers on the network could potentially assign incorrect IP information to devices, disrupting network traffic and potentially redirecting traffic to malicious sites. The presence of student devices may also potentially lead to accidental misconfiguration of DHCP servers in this environment.

Vulnerability 4: ARP Messages are Unverified

ARP messages are not monitored through methods such as dynamic ARP inspection, thus allowing ARP messages to be observed and accepted without verification of their legitimacy. This leads to the LAN being exposed to ARP spoofing attacks, where an attacker might reply to an ARP request with a falsely assigned MAC address, causing traffic to be modified or redirected. Due to the flat nature of the network, this vulnerability may lead traffic to important devices such as the server device being redirected.

Vulnerability 5: Lack of Access Control

The network does not enforce access control lists to restrict what traffic is allowed between specific types of devices. As a result, all devices have unrestricted access to all other devices on the network and all network resources. For example, student devices are able to communicate directly with administrative workstations and teacher devices, again increasing the risk of the exposure of sensitive data, such as academic records.

Vulnerability 6: Lack of Physical Security Measures

Important devices in the network, including the managed switch and the server, are located in closets which are unlocked during school hours and have no other security measures. Physical access to these critical devices allows attackers to bypass any security measures which might be enforced logically on the network completely and allows for tampering with device

configurations. In a school, due to the high amount of individuals present daily, unsecured hardware increases the risk of both accidental and intentional tampering with network devices, such as theft, unplugging devices, and connecting unauthorized hosts.

Most Dangerous Vulnerability:

The most dangerous vulnerability in this network is the flat network architecture. This vulnerability has a high risk because every device which is connected to the network, regardless of its intended permissions and authorization, has the same level of access to other devices. In a school environment, any compromised device is potentially able to attack systems containing sensitive information, and lateral movement is enabled. This vulnerability is primarily reduced by VLAN segmentation since it forces traffic between different VLANs to pass through the network switch. Access control lists, DHCP snooping, and dynamic ARP inspection also limit this vulnerability by limiting what devices can obtain access to the network and mitigating ARP spoofing.

4. Recommended Security Controls & Justification

Control 1: VLAN Segmentation

VLAN segmentation addresses the vulnerability of flat network architecture. VLAN segmentation divides the flat network into multiple virtual subnets, with each subnet containing a separate broadcast domain. As a result, devices within each VLAN will not be able to reach devices in other VLANs without manual configuration, reducing visibility between devices and reducing the possibility of lateral movement. It is recommended that a separate VLAN be created for each of the following: student devices, teacher devices, administrative workstations, the server.

Control 2: Port Security

Enabling port security addresses the lack of security measures taken in physical ports. Port security will limit which devices are allowed to use switch ports by allowing only devices with verified MAC addresses to connect, mitigating the risk of unauthorized access. If unknown devices are connected to the respective ports, then the port will be disabled.

Control 3: DHCP Snooping

DHCP snooping addresses non-restricted DHCP services. DHCP snooping allows DHCP offers only on designated ports on the switch which are confirmed to be trusted, mitigating the possibility of DHCP offers being sent from other ports. This security measure will make DHCP

messages more trustworthy, mitigating the possibility of rogue DHCP servers being introduced. The creation of a table mapping IP addresses to trusted MAC addresses also reduces the risk of ARP spoofing.

Control 4: Dynamic ARP Inspection

Dynamic ARP inspection addresses the lack of verification present for ARP messages. Dynamic ARP inspection requires the binding table created via DHCP snooping, using the binding table to validate ARP messages. Any inconsistent ARP messages will be blocked due to misalignment with the binding table, mitigating the risk of ARP spoofing and unauthorized devices connecting to the network.

Control 5: Access Control Lists

Access control lists enforce access control on the network. Specifically, they provide additional security in local device interactions by defining which hosts are permitted to communicate with each other. This security measure mitigates the risk of unauthorized communication between devices.

Control 6: Physical Security Measures

Physical security measures, such as locks on network closets, identity verification, and monitoring via security cameras, ensure that network equipment is difficult to access and tamper with, whether intentionally or unintentionally. The implementation of keys or security badges to gain access to important network devices mitigates the risk of damage to the network and its devices, as well as hacking and theft.

ACL Intent Statements:

1. Students cannot access the Server, Teacher, and Admin VLANs
2. Teachers have monitored and restricted access to the Server and Student VLANs
3. Only pre-defined MAC addresses are allowed access to a port and assigned an IP address
4. MAC addresses which are not pre-defined are blocked on all ports and not assigned an IP address
5. Only the DHCP server from the server device is trusted for DHCP offers
6. The Server VLAN has access to all VLANs
7. The Admin VLAN has access to the Student and Teacher VLANs

Why VLANs and DHCP Snooping Belong Together:

VLANs and DHCP snooping belong together because VLAN segmentation does not confirm trust in the network, failing to prevent compromised devices inside a respective VLAN from being detected and managed. Although VLANs separate devices into respective broadcast domains and limit communication, a lack of DHCP snooping could cause any device to issue fake DHCP assignments and responses, potentially redirecting the traffic of devices in the VLAN. Since DHCP snooping ensures that only verified DHCP servers can assign IP addresses, it mitigates the possibility of attackers claiming to be an authorized device and redirecting traffic to and from that device. Together, VLAN segmentation is able to limit how many devices an attacker is able to compromise, and DHCP snooping mitigates the risk of an attacker compromising a device in the first place.

5. High-Level Redesign or Improvement Strategy

The proposed network redesign involves VLAN segmentation by role in the network as follows:

VLAN 10: Students
VLAN 20: Teachers
VLAN 30: Admin
VLAN 40: Server

Travel paths will be restricted between the managed switch and the admin workstation VLAN, and between the managed switch and the server VLAN, to ensure that only permitted traffic is allowed.

See **Appendix D** for a visualization of the proposed network redesign.

In the school environment, segmented VLANs generally reduce the visibility of data between devices by logically separating the network into several broadcast ranges. This limits any unnecessary exposure of network information. By assigning devices to a respective VLAN, lateral network to other VLANs is restricted because any data sent between devices in separate VLANs must pass through the managed switch, which enforces access rules. Thus, if a compromised device is introduced to the network, it is less likely to be able to reach sensitive systems such as the admin workstation and the server.

6. Risk Prioritization & Implementation Order

The three controls which should be implemented first are respectively: physical security of network infrastructure, VLAN segmentation, and DHCP snooping.

Physical security is a high priority because gaining physical access allows attackers to bypass all controls enforced via device configurations. The current physical security of the

network allows for unsupervised and unauthorized access of switches and servers, leaving a high risk of compromise. Physical security enforcement reduces the risk of tampering with the hardware and changes in device configuration, as well as the risk of network connectivity issues. If not deployed, attackers can breach the other controls via direct access to privileged network devices.

VLAN segmentation is also of a high priority because it addresses the risk of a lateral movement throughout the entire network by any device. VLAN segmentation allows for the enforcement of various other controls, such as dynamic ARP inspection and access control lists, so its presence is necessary for logical security measures to be effective. VLAN segmentation reduces the risk of lateral movement from compromised or unauthorized host devices to important information and devices. If VLAN segmentation is not deployed, compromised devices may directly access administrative systems, and any breach in the network will compromise the entire network.

DHCP snooping has a high priority because it is required for dynamic ARP inspection and mitigates the risk of the entire network being compromised by the false assignment of IP addresses to devices. DHCP snooping reduces the risk of rogue DHCP servers issuing incorrect IP information or incorrectly resolving DNS. In general, DHCP snooping mitigates the interception and possible redirection of network traffic, If it is not deployed, devices have the ability to completely redirect network traffic or affect its integrity. A lack of DHCP snooping also prevents dynamic ARP inspection from being used safely.

7. Conclusion

The proposed network redesign heavily improves the security of the school's LAN by mitigating unrestricted access, both physically and logically. With the introduction of VLAN segmentation by device category, as well as physical security controls and logical controls such as DHCP snooping and dynamic ARP inspection, the network is secured and monitored. Devices no longer have full access to other network devices, greatly reducing the risk of unauthorized access.

A layered security approach is necessary because one control alone is not able to protect the entire network. The respective controls are designed to handle the risks which other controls fail to address. Physical security controls protect the hardware of the network and ensure that other controls are more difficult to bypass. VLAN segmentation limits the visibility between devices in the network and allows for several other controls which protect against network-based attacks. In general, if one control fails, the other controls may reduce the gravity of the attack.

No single control is sufficient on its own because there are usually methods to either manipulate the infrastructure of the control or bypass it completely. For example, dynamic ARP inspection cannot function without the control of DHCP snooping because the mapping of IP addresses to MAC addresses is necessary for DAI to be successfully executed. Any of the logical

controls also do not address the threat of physical access to the network. Thus, combining these controls allows for stronger security and the minimization of risk.

Appendix

Appendix A - Output of “ip addr” and “ip route”

```
ubuntu@ubuntu:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1
000
    link/ether a2:60:90:be:1f:00 brd ff:ff:ff:ff:ff:ff
    altname enxa26090be1f00
    inet 10.12.18.128/20 brd 10.12.31.255 scope global dynamic noprefixroute enp0s1
       valid_lft 3362sec preferred_lft 3362sec
    inet6 fe80::a060:90ff:febe:1f00/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
ubuntu@ubuntu:~$ ip route
default via 10.12.16.1 dev enp0s1 proto dhcp src 10.12.18.128 metric 100
10.12.16.0/20 dev enp0s1 proto kernel scope link src 10.12.18.128 metric 100
```

Appendix B - Execution and Response of “arping”

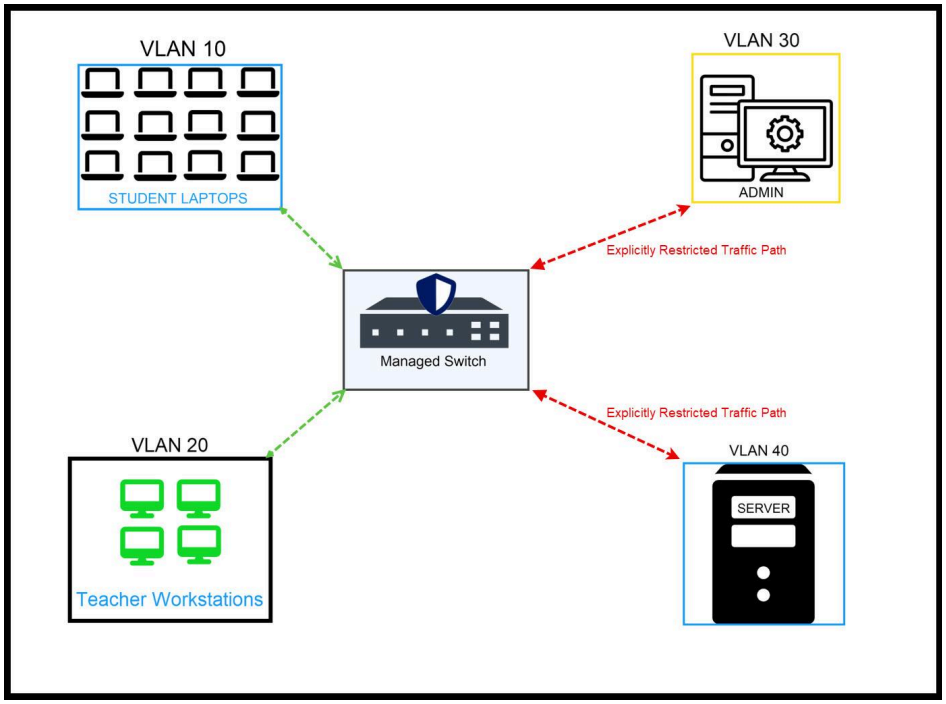
```
ubuntu@ubuntu:~$ sudo arping -c 5 -I enp0s1 10.12.18.128
ARPING 10.12.18.128
42 bytes from a2:60:90:be:1f:00 (10.12.18.128): index=0 time=417.331 usec
42 bytes from a2:60:90:be:1f:00 (10.12.18.128): index=1 time=1.149 msec
42 bytes from a2:60:90:be:1f:00 (10.12.18.128): index=2 time=981.202 usec
42 bytes from a2:60:90:be:1f:00 (10.12.18.128): index=3 time=882.078 usec
42 bytes from a2:60:90:be:1f:00 (10.12.18.128): index=4 time=1.068 msec

--- 10.12.18.128 statistics ---
5 packets transmitted, 5 packets received,   0% unanswered (0 extra)
rtt min/avg/max/std-dev = 0.417/0.900/1.149/0.257 ms
```

Appendix C - Arp Requests Shown on Server Computer

```
15:39:10.610293 ARP, Request who-has MaryBuwicksAir.cls-edu.charlottelatin.org tell 10.12.26.25, l
ength 44
15:39:10.610314 ARP, Reply MaryBuwicksAir.cls-edu.charlottelatin.org is-at a2:60:90:be:1f:00 (oui
Unknown), length 28
15:39:11.614466 ARP, Request who-has MaryBuwicksAir.cls-edu.charlottelatin.org tell 10.12.26.25, l
ength 44
15:39:11.614514 ARP, Reply MaryBuwicksAir.cls-edu.charlottelatin.org is-at a2:60:90:be:1f:00 (oui
Unknown), length 28
15:39:12.618430 ARP, Request who-has MaryBuwicksAir.cls-edu.charlottelatin.org tell 10.12.26.25, l
ength 44
15:39:12.618466 ARP, Reply MaryBuwicksAir.cls-edu.charlottelatin.org is-at a2:60:90:be:1f:00 (oui
Unknown), length 28
15:39:12.692426 ARP, Request who-has JTStreamingMBP.cls-edu.charlottelatin.org tell 10.12.26.128,
length 28
15:39:13.623705 ARP, Request who-has MaryBuwicksAir.cls-edu.charlottelatin.org tell 10.12.26.25, l
ength 44
15:39:13.623739 ARP, Reply MaryBuwicksAir.cls-edu.charlottelatin.org is-at a2:60:90:be:1f:00 (oui
Unknown), length 28
15:39:14.626028 ARP, Request who-has MaryBuwicksAir.cls-edu.charlottelatin.org tell 10.12.26.25, l
ength 44
15:39:14.626073 ARP, Reply MaryBuwicksAir.cls-edu.charlottelatin.org is-at a2:60:90:be:1f:00 (oui
Unknown), length 28
15:39:21.301050 ARP, Request who-has _gateway tell 10.12.26.128, length 28
```

Appendix D - Proposed Network Segmentation Plan


VLAN 10
STUDENT LAPTOPS
VLAN 30
ADMIN
Explicitly Restricted Traffic Path
Managed Switch
Explicitly Restricted Traffic Path
VLAN 20
Teacher Workstations
VLAN 40
SERVER