Project One: Segmentation

Dennis Tria

Department of Information Technology, SNHU

CYB 210 Computer Networking

Professor Erick Rivers

August 08, 2025

**Introduction**

This project reconfigured the Department of Motor Vehicles (DMV) network to provide open guest wireless internet and enhance physical security with surveillance cameras, ensuring secure and isolated traffic flow. Using Cisco Packet Tracer, I implemented VLAN segmentation, DHCP services, and IP addressing to meet these requirements, aligning with industry best practices for small to medium-sized enterprise networks as outlined in Cisco’s network segmentation guidelines (Cisco, 2023). The solution demonstrates mastery of competencies: *implementing IP addressing and supporting services* (e.g., DHCP, static IPs) and *configuring common network functions and devices* (e.g., switch VLANs, router DHCP) to meet architectural needs, creating a scalable and secure network tailored to the DMV’s operational goals.

**A. How Network Traffic Was Segmented**

To safeguard DMV sensitive data and comply with security standards (e.g., HIPAA or PCI-DSS), I segmented the network using VLANs on a Cisco 2960-24TT switch. Network segmentation improves performance by reducing congestion and enhances security by limiting attack spread, aligning with Cisco’s recommendation to isolate traffic types for operational efficiency and protection (Cisco, 2023). This was critical for the DMV to prevent guest users from accessing internal systems and to ensure surveillance feeds remained private.

I began by issuing show vlan brief to establish a baseline of existing VLANs and port assignments, ensuring no critical configurations (e.g., VLAN 50 Data) Ire overwritten—a proactive step to maintain network stability. The topology was physically arranged in Packet Tracer to reflect logical segmentation:

* **Video Camera Area (VLAN 80)**: Ibcam Lobby and Ibcam Door for secure surveillance.
* **Guest Wireless Area (VLAN 70)**: Smartphone and Tablet for customer Wi-Fi.
* **Workstations (VLAN 50)**: PC1 (192.168.50.5) and PC2 (192.168.50.6) for internal operations.

VLAN Setup

I created VLANs to isolate traffic, enhance security and compliance:

enable

configure terminal

vlan 50

name Data

vlan 70

name Guest

vlan 80

name Video

vlan 150

name Voice

exit

end

After creating the VLANs, I verified that they Ire properly configured and active by running the show vlan brief command. This command displays a summary of all VLANs, including their names, status, and assigned ports, allowing us to confirm the setup before proceeding with port assignments and device connections.

Verification used:

show vlan brief

Sample output (screenshot: VLAN\_Configuration.png):

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN | Name | Status | Ports |
| 1 | default | active | Fa0/1, Fa0/2, Fa0/4, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/16, Fa0/17, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig0/1, Gig0/2 |
| 50 | Data | active | Fa0/5, Fa0/6 |
| 70 | Guest | active | Fa0/3 |
| 80 | Video | active | Fa0/18, Fa0/19 |
| 150 | Voice | active | Fa0/15 |

This setup isolates traffic, reducing compliance scope to in-scope systems (e.g., VLAN 80 cameras). The table below summarizes VLAN purposes, ports, and devices for clarity:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VLAN | Name | Purpose | Ports | Devices/IPs |
| 50 | Data | Workstations | Fa0/5, Fa0/6 | PC1: 192.168.50.5, PC2: 192.168.50.6 |
| 70 | Guest | Wireless | Fa0/3 | Smartphone: 192.168.70.10, Tablet: 192.168.70.12 |
| 80 | Video | Cameras | Fa0/18, Fa0/19 | Lobby: 192.168.80.10, Door: 192.168.80.11 |
| 150 | Voice | Future VoIP | Fa0/15 | None (reserved) |

**Device Configuration: Cameras**

To ensure reliable surveillance and protect vulnerable devices, I assigned static IPs to cameras on VLAN 80:

* **Lobby Ibcam**: 192.168.80.10, connected to Fa0/18.
* **Door Ibcam**: 192.168.80.11, connected to Fa0/19.

Connections used copper straight-through cables for high-speed links. Configuration:

1. Go to Config tab > FastEthernet interface.
2. Set static IP (192.168.80.10 or .11, subnet 255.255.255.0).

Ports Ire assigned:

interface range fa0/18 - 19

switchport mode access

switchport access vlan 80

end

(screenshot: Switch\_VLAN80\_Config.png). This isolates camera traffic, preventing interference and enhancing security.

**Device Configuration: Wireless + DHCP**

To provide accessible guest Wi-Fi while protecting internal resources, I configured the WRT300N router for VLAN 70 with DHCP for dynamic IP assignment, reducing administrative burden. Settings:

* **Router IP**: 192.168.70.1, Subnet: 255.255.255.0.
* **DHCP**: Enabled, Start IP: 192.168.70.10, Max Users: 70, DNS: 8.8.8.8.
* **Wireless**: Mode: Mixed, SSID: Guest\_WiFi, Channel: 1 (2.412GHz), Broadcast: Enabled, Security: Disabled.

(screenshot: DHCP\_Config\_WRT300N.png for DHCP settings).

Device setup for Smartphone (192.168.70.10) and Tablet (192.168.70.12):

1. Config tab > Wireless0.
2. Set SSID: Guest\_WiFi, Authentication: Open, IP config: DHCP.

(screenshots: Wireless\_BasicSettings\_GuestWiFi.png, Wireless\_Security\_Disabled.png, Smartphone\_GuestWiFi\_IP.png, Tablet\_GuestWiFi\_IP.png).

**Router–Switch Connection**

To enable DHCP and isolate guest traffic, I connected switch Fa0/3 to router Ethernet Port 1 with a copper straight-through cable, ensuring secure routing without exposing internal networks:

interface fa0/3

switchport mode access

switchport access vlan 70

end

copy running-config startup-config

(screenshot: Router\_Port\_VLAN.png). This supports guest access while maintaining segmentation, a key security benefit per Cisco.

**Ping Tests for Verification**

To confirm segmentation and limit cyberattack damage, I conducted ping tests:

* **Lobby (192.168.80.10) ↔ Door (192.168.80.11)**: Successful (0% loss, screenshot: VLAN80\_PingTest\_Success.png), proving intra-VLAN connectivity.
* **Smartphone (192.168.70.10) → Lobby (192.168.80.10)**: Failed (unreachable, screenshot: Ping\_GuestToVideo\_Failed.png).
* **Door → Smartphone (192.168.70.10)**: Failed (timed out, screenshot: Ping\_VideoToGuest\_Failed.png).
* **Smartphone → PC1 (192.168.50.5)**: Failed, reinforcing Data isolation.

(screenshot: Ping\_VideoDevices.png for additional Video success pings).

Troubleshooting camera pings required:

1. Click Advanced > I/O Config.
2. Check "Show Desktop" for Command Prompt.

(screenshots included). This verified isolation, protecting DMV systems from unauthorized access.

**B. Scalability of the Guest Wireless Network**

The Guest VLAN (70) was designed to support up to 70 users for 4 hours, ensuring scalable Wi-Fi access for DMV customers while maintaining security. I used the WRT300N router to manage DHCP, isolating guest traffic to prevent performance degradation or attacks on internal systems, per Cisco’s performance and security benefits (Cisco, 2023).

**DHCP Configuration**

To simplify IP management and support scalability, I configured:

* **Router IP**: 192.168.70.1, Subnet: 255.255.255.0 (254 IPs for future growth).
* **DHCP Range**: 192.168.70.10 to .79 (70 IPs).
* **Max Users**: 70, matching demand.
* **DNS Server**: 8.8.8.8, ensuring reliable internet access.
* **Lease Time**: 0 (24 hours, unchangeable per Packet Tracer).

The /24 subnet was chosen to allow expansion, while the DHCP range limits resource use, aligning with scalability goals (screenshot: DHCP\_Config\_WRT300N.png).

**Wireless Configuration**

To accommodate diverse devices and ensure ease of access:

* **Mode**: Mixed (802.11b/g/n), supporting various client types.
* **SSID**: Guest\_WiFi, clearly identifiable.
* **Broadcast**: Enabled, enhancing discoverability.
* **Security**: Open, per DMV requirements for quick guest access.

(screenshots: Wireless\_BasicSettings\_GuestWiFi.png, Wireless\_Security\_Disabled.png).

**Scalability Benefits**

This setup supports scalability by:

* Using a /24 subnet for future capacity.
* Automating IP assignment with DHCP.
* Isolating VLAN 70 to protect internal traffic.
* Leveraging DNS 8.8.8.8 for scalable internet access.

Troubleshooting APIPA (169.254.x.x) errors involved verifying DHCP and connectivity, ensuring valid IPs (Smartphone: 192.168.70.10, Tablet: 192.168.70.12). This aligns with the DMV’s need for efficient, secure guest services.

**Conclusion**

This project delivered a secure, scalable DMV network by implementing VLAN segmentation to isolate guest, video, and data traffic, preventing unauthorized access and limiting attack spread—key benefits per Cisco’s guidelines (Cisco, 2023). DHCP on the WRT300N supported 70 users with room for growth, while static IPs ensured reliable camera operation. Ping tests and troubleshooting (e.g., camera Desktop tab) verified functionality, showcasing problem-solving skills. This solution reflects competencies in IP addressing (DHCP, static IPs) and device configuration (switch VLANs, router setup), aligning with industry best practices for secure, scalable networks. All configurations, screenshots (VLAN\_Configuration.png, DHCP\_Config\_WRT300N.png, Switch\_VLAN80\_Config.png, Ping\_VideoDevices.png, etc.), and the Packet Tracer .pkt file are submitted separately.

**References**

Cisco. (2023). What Is Network Segmentation? Retrieved from <https://www.cisco.com/site/us/en/learn/topics/security/what-is-network-segmentation.html>