SD-WAN Network Security & Performance

Understanding Congestion and DDoS in Healthcare

Computer Networks Project

January 23, 2026

Scenario: The Digital Hospital

Modern hospitals are digital ecosystems.

- **Radiology**: Sending huge MRI images (Gigabytes).
- **Surgeons**: Video calling colleagues during operations.
- **Patients**: Using Guest Wi-Fi.

The Challenge: How do we keep the surgeon's video smooth when a patient starts downloading a movie?

What is SD-WAN?

Traditional WAN vs SD-WAN

- **Traditional**: Like a train on fixed tracks. Can't change route if there's a jam.
- **SD-WAN**: Like a GPS app (Waze/Google Maps). Sees traffic in real-time and steers data to the fastest open road.

The Danger: Congestion vs. DDoS

- **1. Legitimate Congestion**:
  - **Cause**: Too much good work happening (e.g., 3 Doctors opening X-Rays).
  - **Action**: **Queue it. Prioritize it.**

- **2. DDoS Attack**:
  - **Cause**: Malicious Hackers / Botnets.
  - **Action**: **Block it immediately.**

Misidentifying them is dangerous!

Traffic Priority (QoS)

Class	Traffic	Priority	Examples
GOLD	Real-time	High	VoIP, Tele-surgery
SILVER	Business	Medium	EMR, MRI Scans
BRONZE	Best Effort	Low	YouTube, Guest Wi-Fi

Solution: Weighted Fair Queuing (WFQ)

Imagine a Club Entrance with 3 Lines:

- **Gold Line (VIP)**: Lets 6 people in.
- **Silver Line**: Lets 3 people in.
- **Bronze Line**: Lets 1 person in.

Even if the Bronze line has 1000 people, the VIPs still get through quickly.

Conclusion

1. We use **Mathematics** (Entropy) to detect attacks.
2. We use **QoS Queuing** to protect critical patient data.
3. Real-time analysis gives us visibility.