📦 Packet Generation & Analysis Lab

This guide will teach you how to generate different types of network traffic between Mininet hosts. We will move beyond simple ping and use professional tools.

🛠️ Step 1: Installation & Setup

Before we start Mininet, we need to make sure our tools are installed on your Linux system.

1. Install the Tools:
   Open your main terminal and run:
   sudo apt-get update
   sudo apt-get install iperf3 hping3
   # Note: D-ITG often requires manual compilation.
   # For this lab, we will focus on Iperf and Hping3,
   # but instructions for D-ITG are included if your VM supports it.

2. Start Mininet:
   We need a simple setup: One sender (Client) and one Receiver (Server).
   sudo mn --topo single,2

3. Open Terminals:
   Inside Mininet (mininet>), open terminals for both hosts:
   xterm h1 h2

   - **h1 (10.0.0.1):** The Sender (Generator)
   - **h2 (10.0.0.2):** The Receiver (Target)

🚀 Tool 1: Iperf3 (The Speed Tester)

Best for: Measuring maximum bandwidth and throughput.
Concept: h2 acts as a bucket, and h1 tries to fill it with water (data) as fast as possible.
1. Set up the Server (h2):
In the h2 terminal, tell it to listen for incoming data.
iperf3 -s

(It is now waiting...)

2. Start the Generator (h1):
In the h1 terminal, fire the packets at h2.
-c: Client mode (connect to 10.0.0.2)
-t: Time (run for 10 seconds)
iperf3 -c 10.0.0.2 -t 10

3. Analyze:
Look at the output. You will see "Transfer" (how much data moved) and "Bitrate" (the speed). In Mininet, this should be very high (Gbps).

🎭 Tool 2: Hping3 (The Custom Crafter)

Best for: Security testing and creating specific TCP/IP flags.
Concept: Unlike Iperf which sends random data, Hping3 lets you build the packet by hand (e.g., "Send a TCP SYN packet to port 80").
1. The SYN Flood (h1):
Let's try to send a stream of connection requests (SYN) to h2.

```
# -S: Set SYN flag
# -p 80: Target port 80
# --flood: Send as fast as possible (Be careful!)
hping3 -S -p 80 --flood 10.0.0.2
```

2. Stop it:
Press Ctrl+C quickly.
3. Analyze:
You will see a summary of how many packets were transmitted. This is often used to test how firewalls handle high packet loads.

📊 Tool 3: D-ITG (The Realism Mimic)

Best for: Simulating real-world apps like VoIP or Telnet.
Concept: Iperf just sends "data." D-ITG sends data with the specific timing and pauses of a real human conversation or video stream.
(Note: If D-ITG is not in your path, you may need to install the d-itg package specifically).

1. Set up the Receiver (h2):

```
ITGRecv
```

2. Start the Generator (h1):
Let's simulate a UDP stream (like a video call).

```
# -a: Destination Address
# -T: Protocol (UDP)
# -C: Rate (100 packets per second)
# -t: Duration (10000 milliseconds = 10s)
ITGSend -a 10.0.0.2 -T UDP -C 100 -t 10000
```

3. Analyze:
D-ITG creates a log file. It calculates "Jitter" (delay variation) and "Delay," which are critical for voice and video quality.

🧠 Learning Outcomes

1. **Iperf:** Used to check "How big is my pipe?" (Bandwidth).
2. **Hping3:** Used to check "Is the firewall working?" (Stress/Flag testing).
3. **D-ITG:** Used to check "Can this network handle a Skype call?" (QoS/Jitter).