ENSC 427:COMMUNICATION NETWORKS
FALL 2021

Simulation of Distributed and Regular DoS Attack in the Campus Wi-fi Environment

https://ks03ks.wixsite.com/my-site/presentation

Emmanuel Komolafe 301297069
ikomolaf@sfu.ca

Eric Sunmin Kim 301324510
sunmink@sfu.ca

Group 2

Outline

- Introduction
- Overview of Related Work
- Problem Description
- Implementation (Setup, Simulation, and Results)
- Discussion
- References

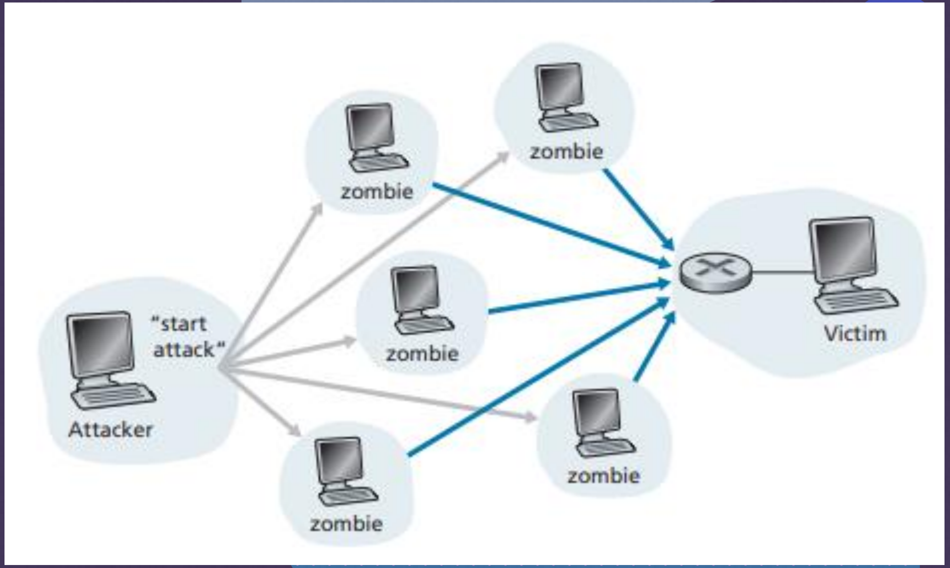
Introduction

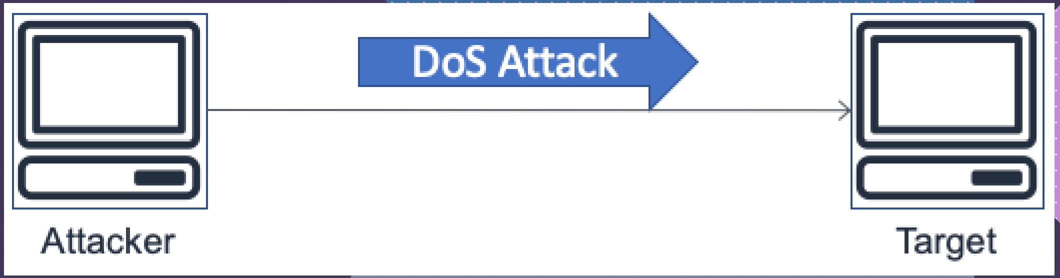
- **Objective**: Simulating the common wi-fi environment with DoS and DDoS attack
- **Motivation**:
- How much difference would DDoS and DoS attack make in the data transferring capability of wi-fi environment?
- Is DoS attack enough to cause detrimental damage to the server?
- **Scope/Overview:**
  - Basic wi-fi network topology
  1. Regular Campus Network Topology
  2. Campus Network Topology with Single Attacker (DoS)
  3. Campus Network Topology with an attacker and Multiple Zombies (DDoS)

What are DoS and DDoS?

- DoS stands for Denial of service
- DDoS stands for Distributed Denial of service
- Both Dos and DDoS are forms of cyber attack to servers
- Difference between DoS and DDoS:

DoS	DDoS
One machine to launch attack to the server	Multiple machines launch the attack to the server
Low threat	Poses a lot of danger
No malware involved here	Consists of numerous infected machines
Tracing source of attack is relatively easier than DDoS	Tracing source of attack is complex because of the use of botnets





Overview of Related Work

- **Simulation of DDoS attacks in 4G networks:** Study of DDoS attack on a 4G network in ns-3

  done by Nathanael Tan, Sharon Makina, and Merna Zaki

- **Effects of Different Topologies on the Content Distribution Network:** study on how different topologies affect the CDN

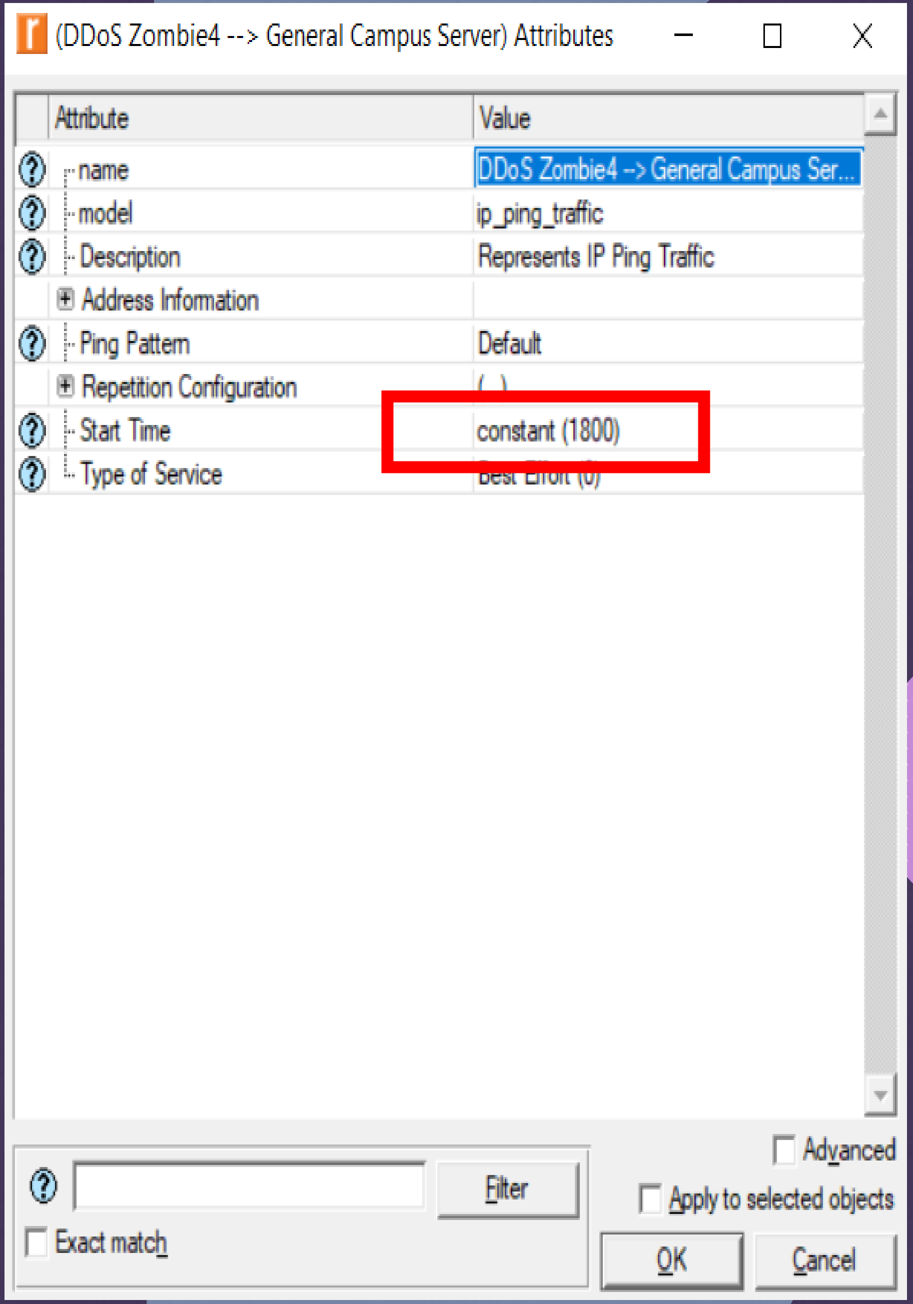
  done by Lance Zhang, Jonsen Li, and Richard Sun

Problem Description

- The effects of DoS and DDoS attack on the network
- 3 different topologies used
  1. Topology without any interference
  2. Topology with a single attacker

     - single attacker initiates attack at 1800 second (30min) with a constant rate
  3. Topology with various attackers (zombies)

     - Five attackers simultaneously initiate attacks at 1800 second (30 min) with a constant rate

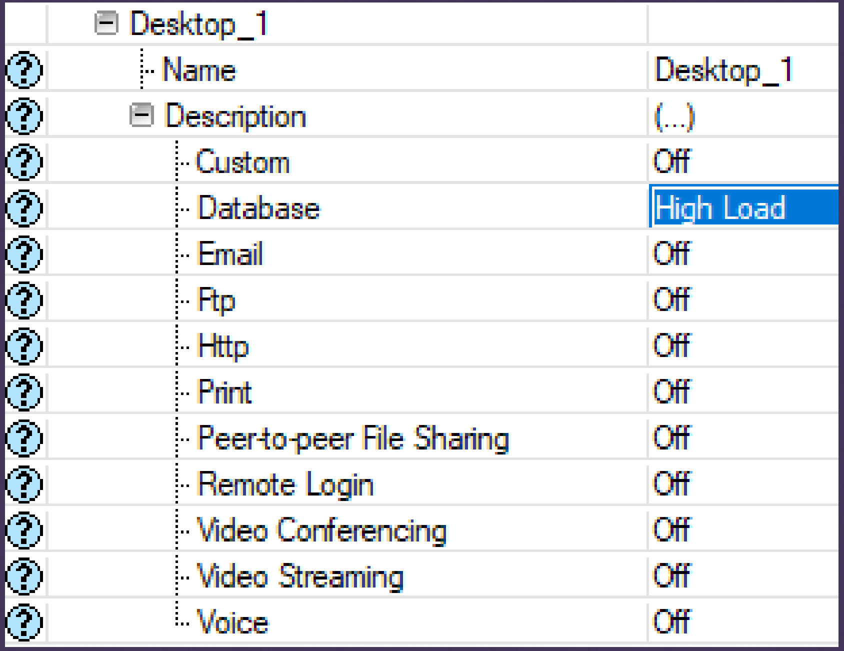


(DDoS Zombie4 --> General Campus Server) Attributes

Attribute	Value
name	DDoS Zombie4 --> General Campus Ser...
model	ip_ping_traffic
Description	Represents IP Ping Traffic
⊞ Address Infomation	
Ping Pattern	Default
⊞ Repetition Configuration	(...)
Start Time	constant (1800)
Type of Service	Best Effort (0)

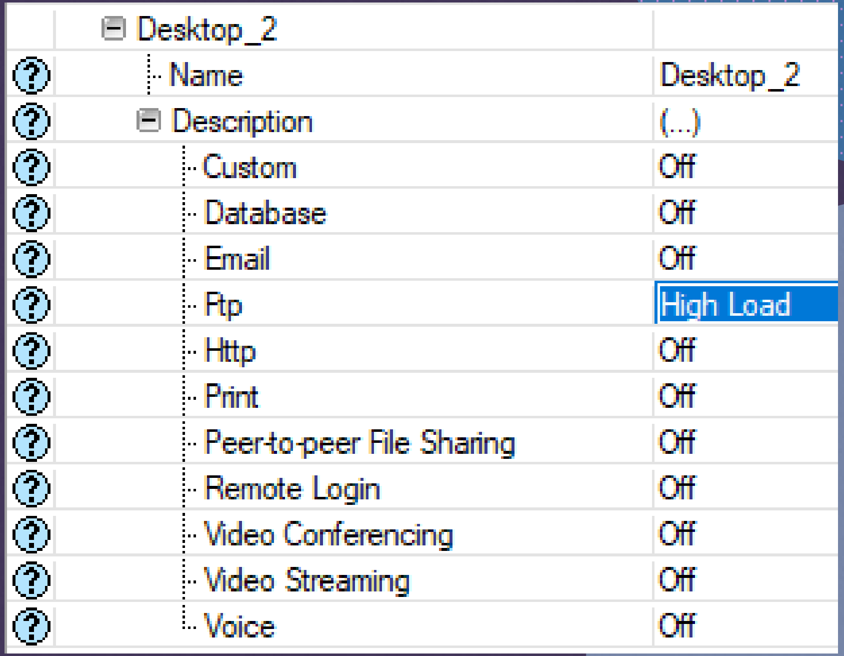
Implementation

- Each Desktop computer is designed in a way that they best represent the real users using commonly-used network applications
- Desktop 1:



⊟ Desktop_1	
Name	Desktop_1
⊟ Description	(...)
Custom	Off
Database	High Load
Email	Off
Ftp	Off
Http	Off
Print	Off
Peer-to-peer File Sharing	Off
Remote Login	Off
Video Conferencing	Off
Video Streaming	Off
Voice	Off

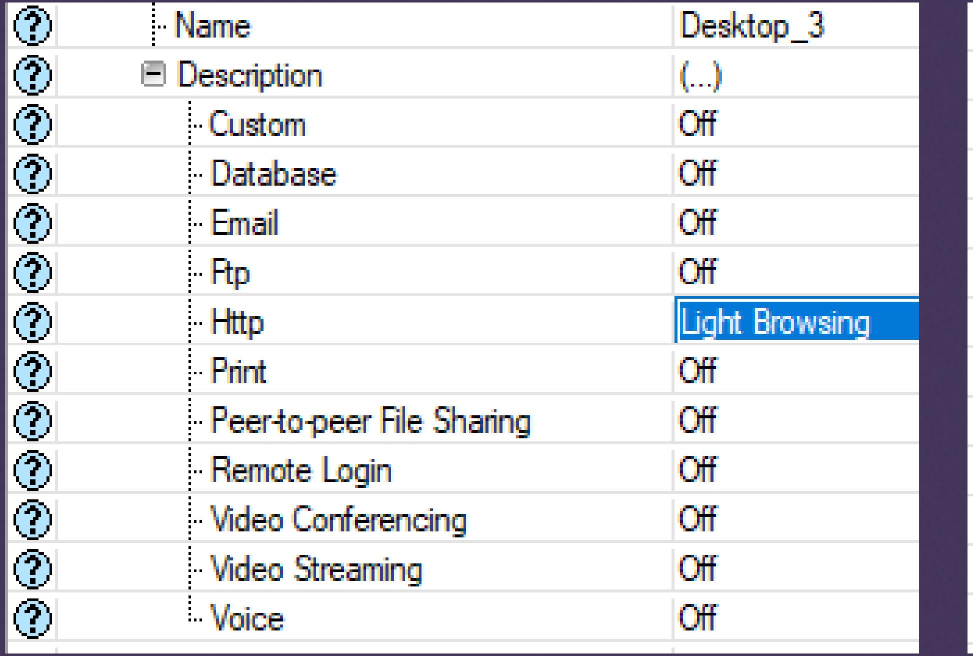
Desktop 2:



⊟ Desktop_2	
Name	Desktop_2
⊟ Description	(...)
Custom	Off
Database	Off
Email	Off
Ftp	High Load
Http	Off
Print	Off
Peer-to-peer File Sharing	Off
Remote Login	Off
Video Conferencing	Off
Video Streaming	Off
Voice	Off

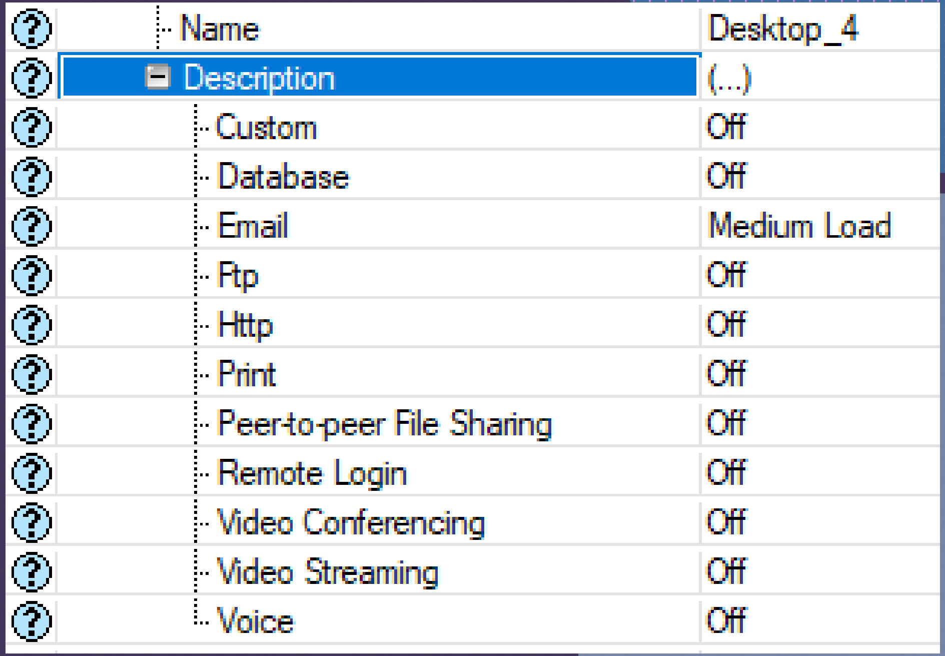
Implementation

- Each Desktop computer is designed in a way that they best represent the real users using commonly-used network applications
- Desktop 3:



Name	Desktop_3
⊟ Description	(...)
Custom	Off
Database	Off
Email	Off
Ftp	Off
Http	Light Browsing
Print	Off
Peer-to-peer File Sharing	Off
Remote Login	Off
Video Conferencing	Off
Video Streaming	Off
Voice	Off

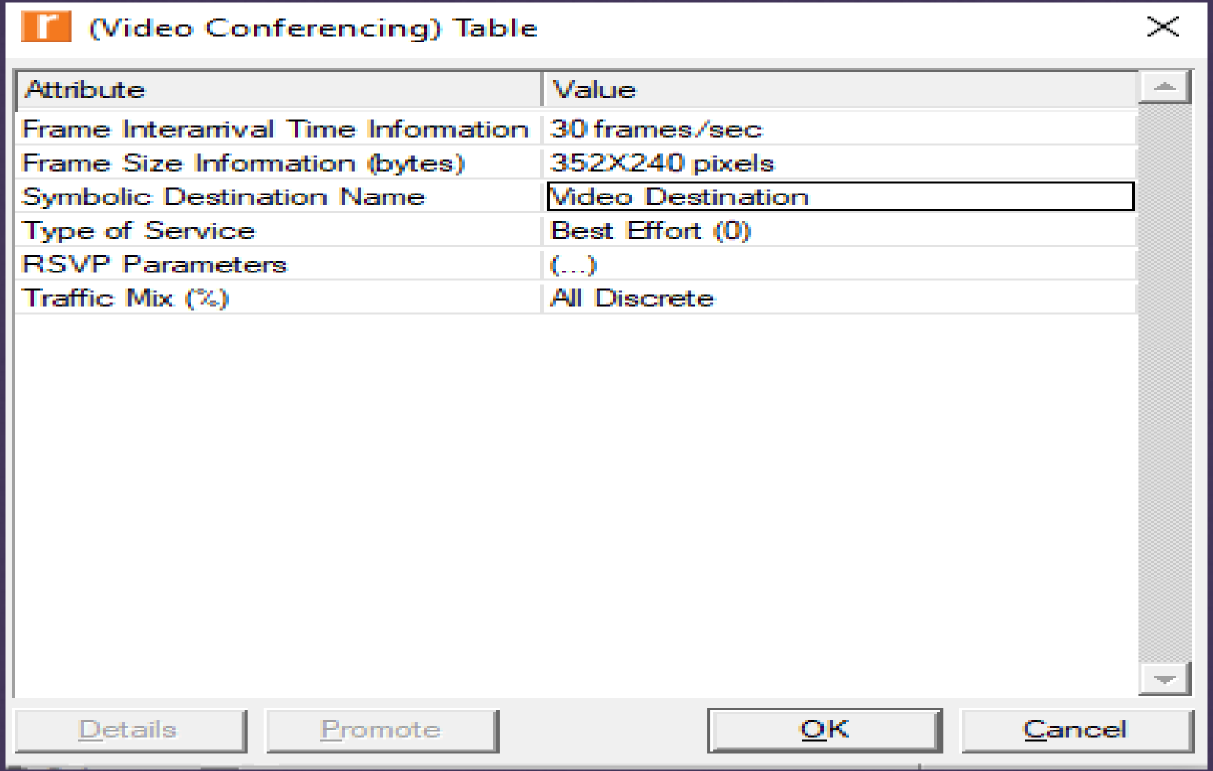
Desktop 4:



Name	Desktop_4
⊟ Description	(...)
Custom	Off
Database	Off
Email	Medium Load
Ftp	Off
Http	Off
Print	Off
Peer-to-peer File Sharing	Off
Remote Login	Off
Video Conferencing	Off
Video Streaming	Off
Voice	Off

Implementation

- Each Desktop computer is designed in a way that they best represent the real users using commonly-used network applications
- Desktop 5:

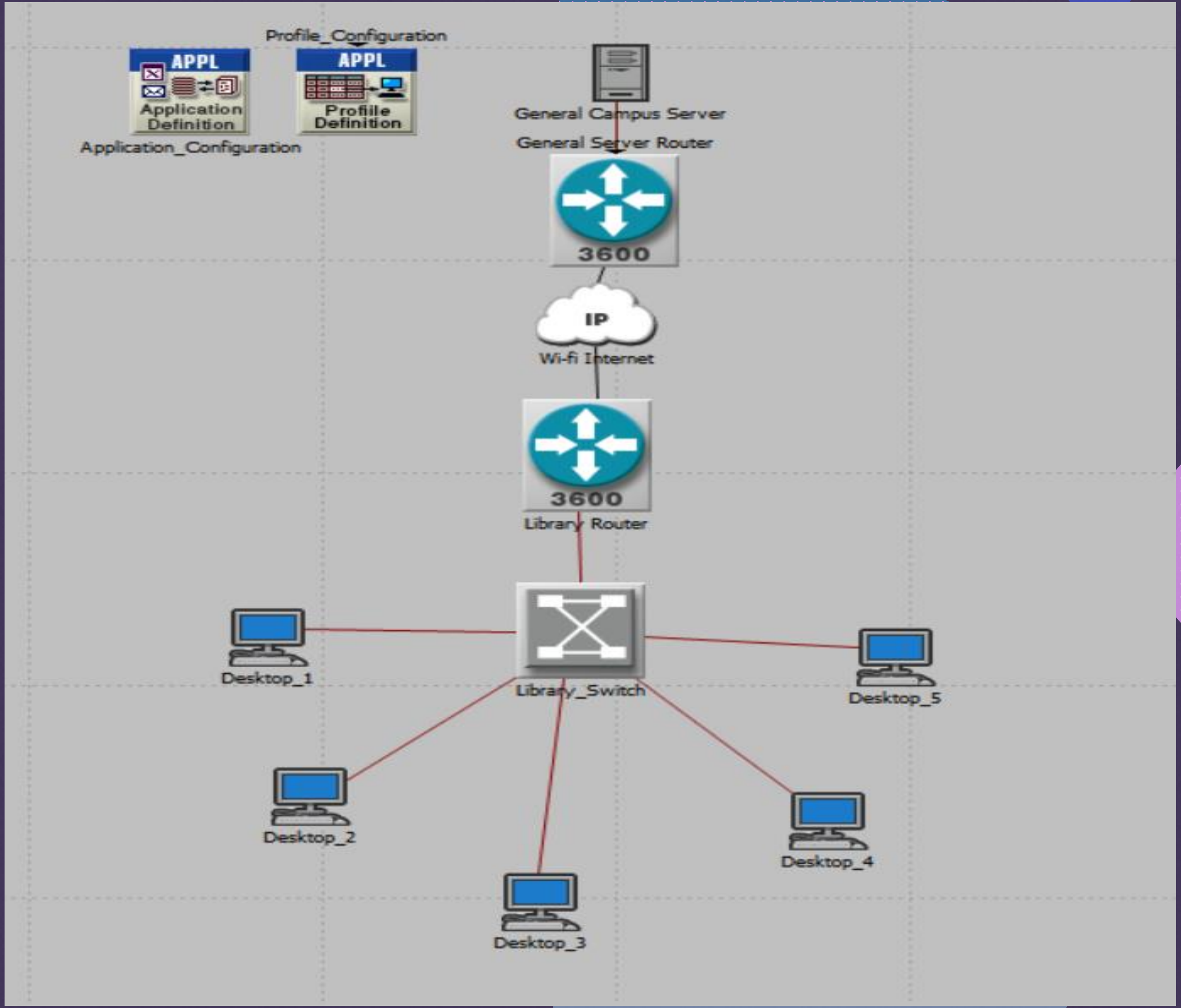


(Video Conferencing) Table

Attribute	Value
Frame Interarrival Time Information	30 frames/sec
Frame Size Information (bytes)	352X240 pixels
Symbolic Destination Name	Video Destination
Type of Service	Best Effort (0)
RSVP Parameters	(...)
Traffic Mix (%)	All Discrete

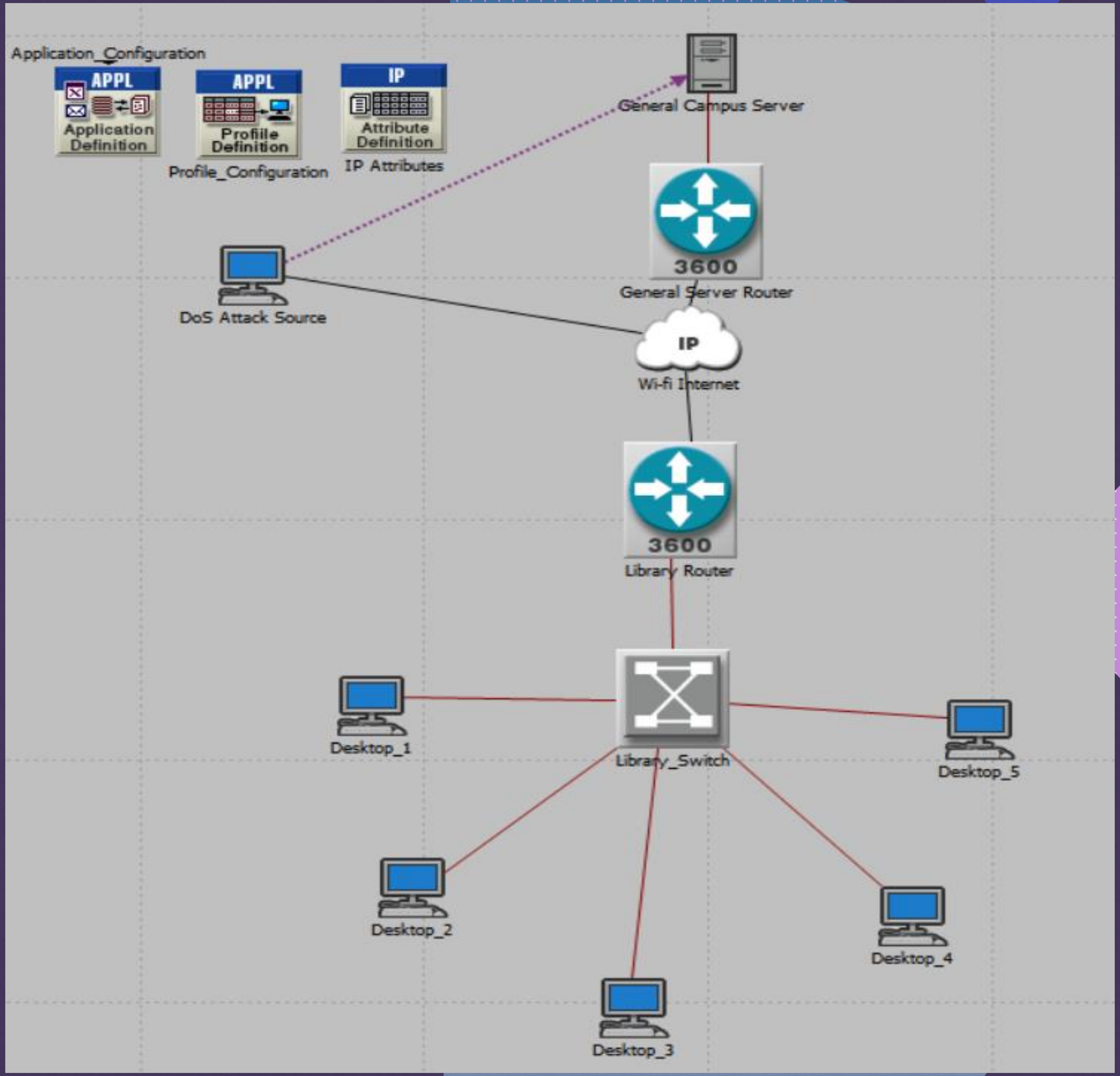
Network Topology Setup (Normal Event)

- The simulated network topology of campus library network
- 5 workstations in the library connected to the switch
- One switch, one Cisco router are used in this campus network



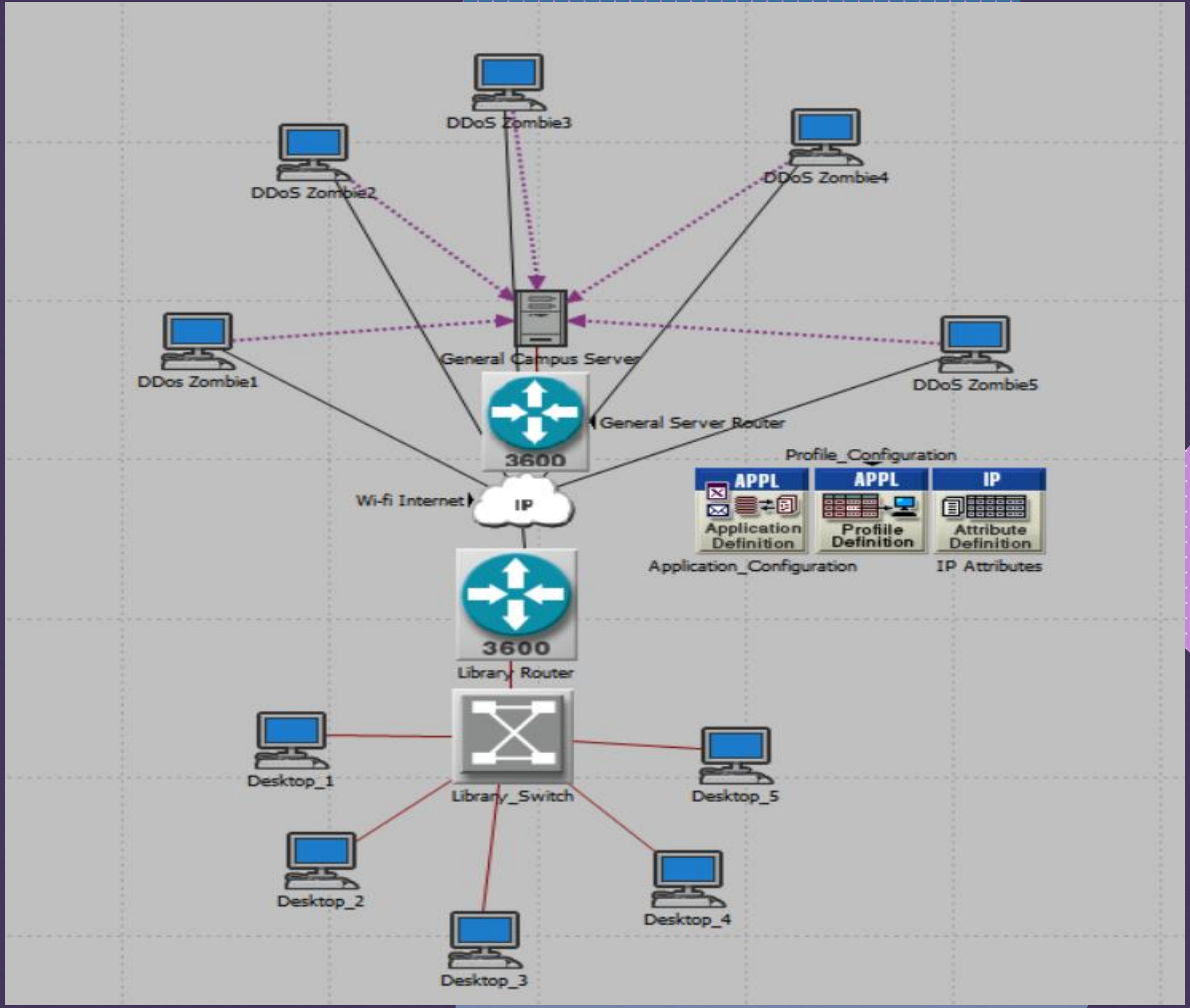
Network Topology Setup (DoS)

- The simulated network topology of campus library network with a single attacker
- Standalone attacker introduced by using IP ping traffic link to the server
- IP ping parameters:
  - Packet size 65,527 bytes
  - IPv4

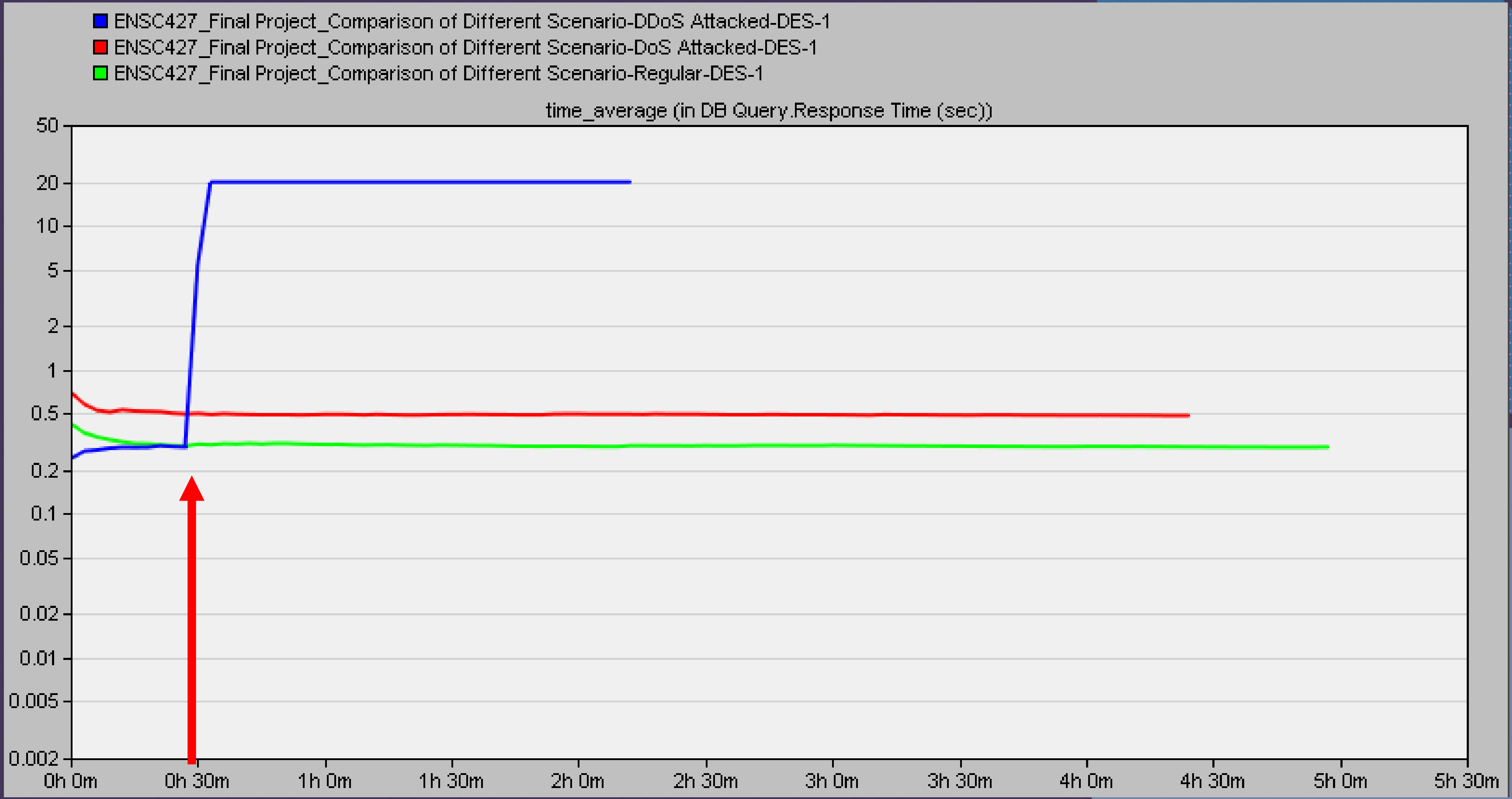


Network Topology Setup (DDoS)

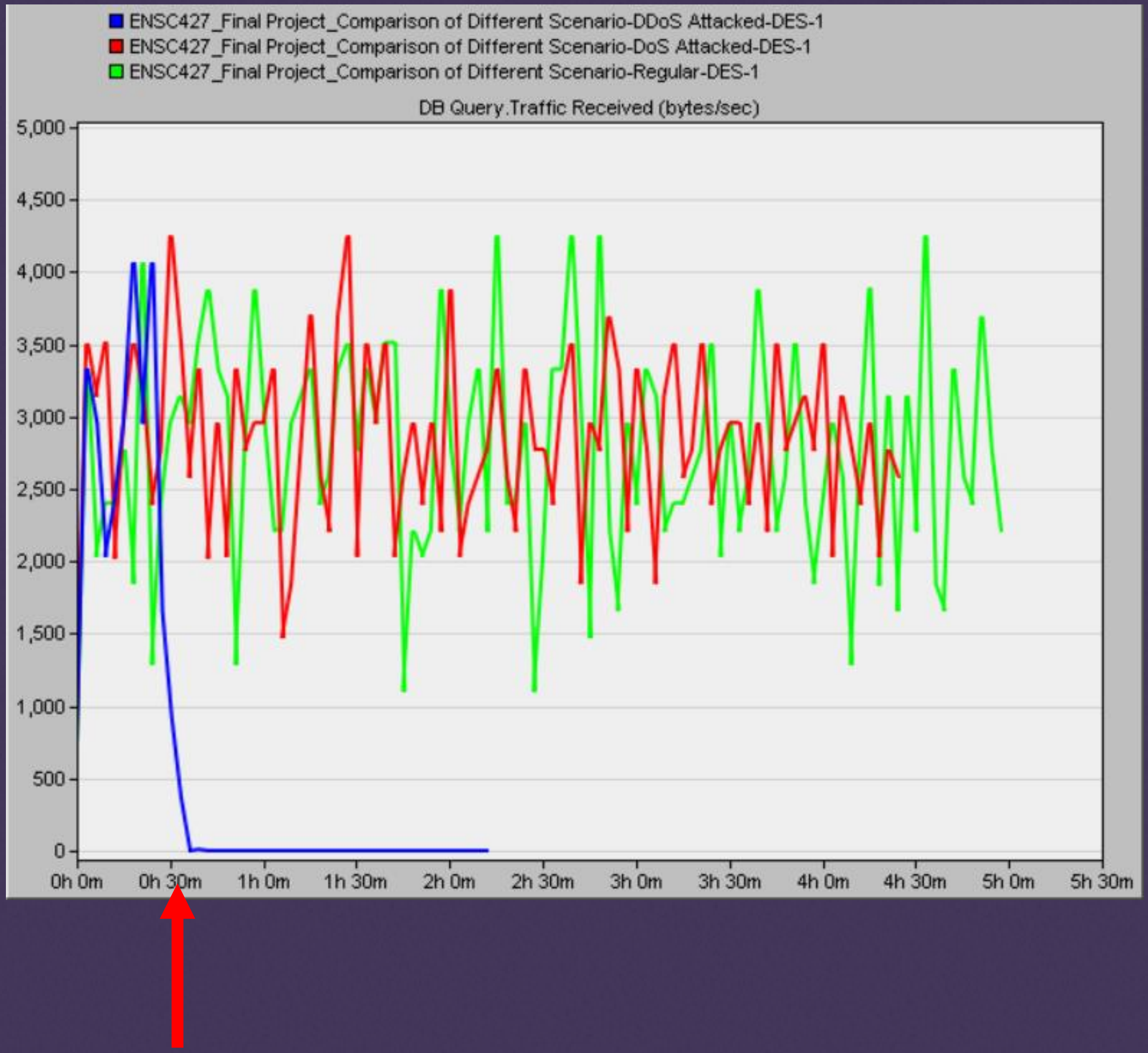
- The simulated network topology of campus library network with five attackers
- Four additional attackers (zombies) are introduced to increase the pressure
- The additional zombies are connected to the server

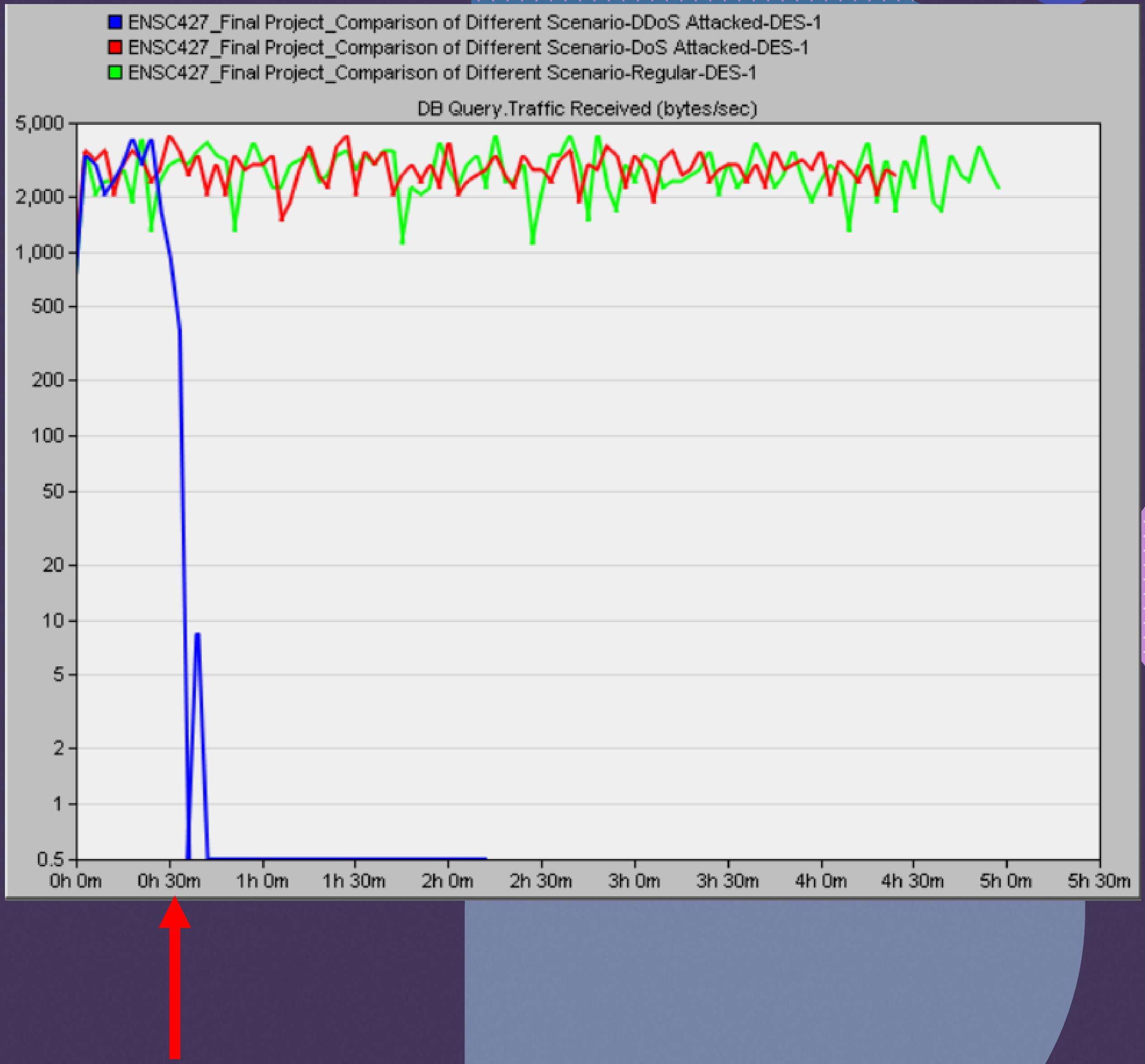


Simulation Results (DB Query Response Time)

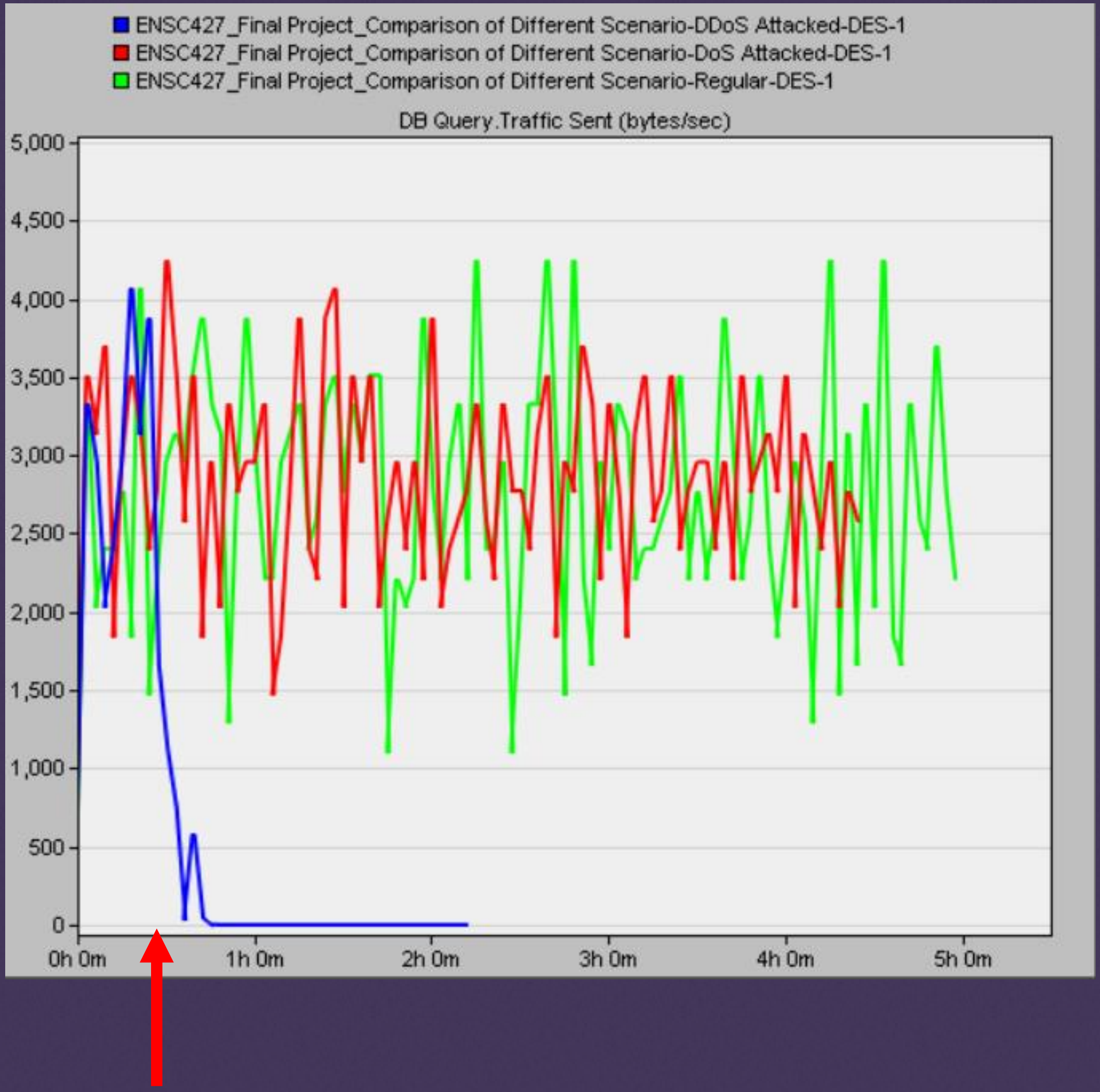


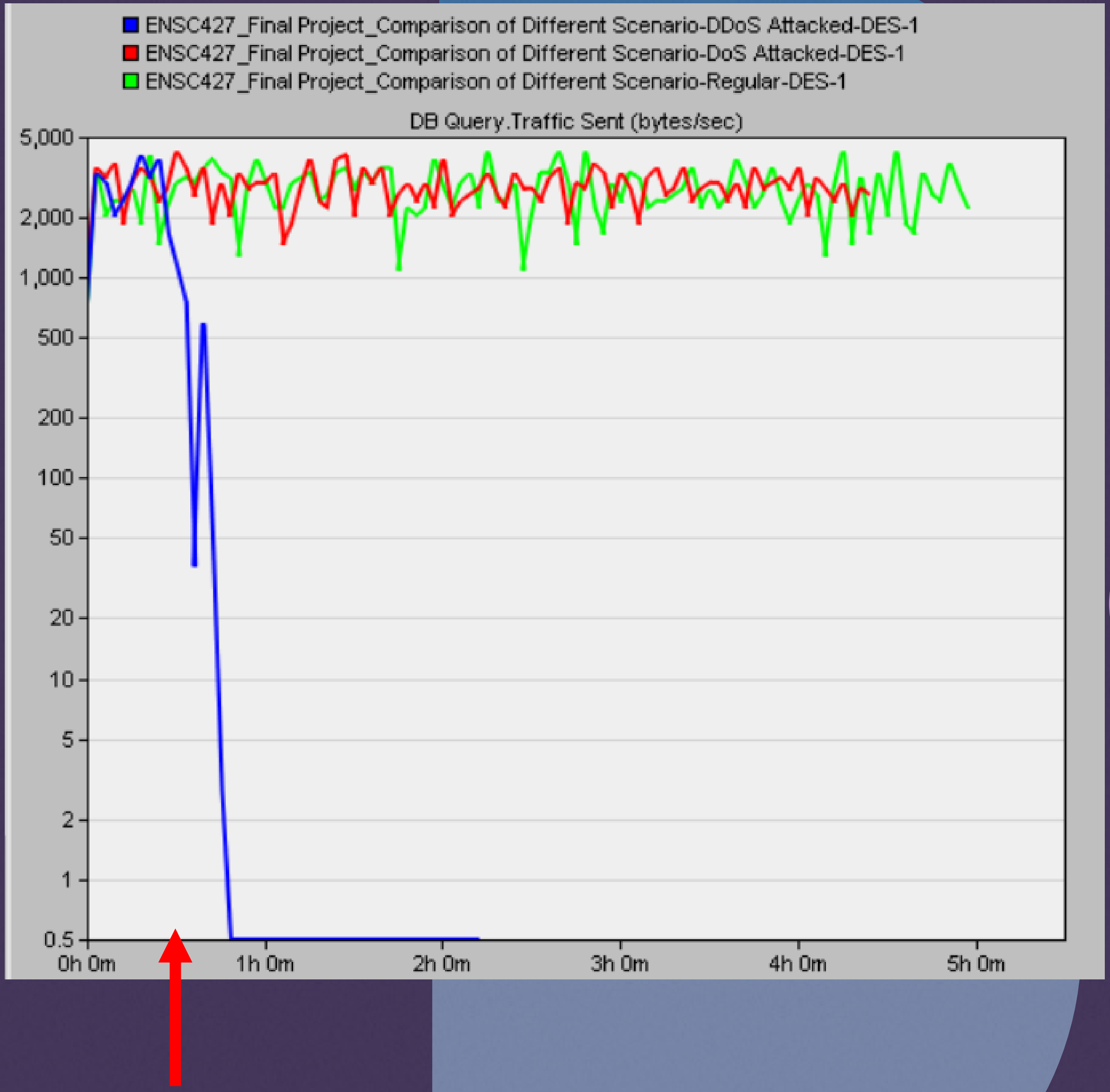
Simulation Results (DB Query Traffic Received)



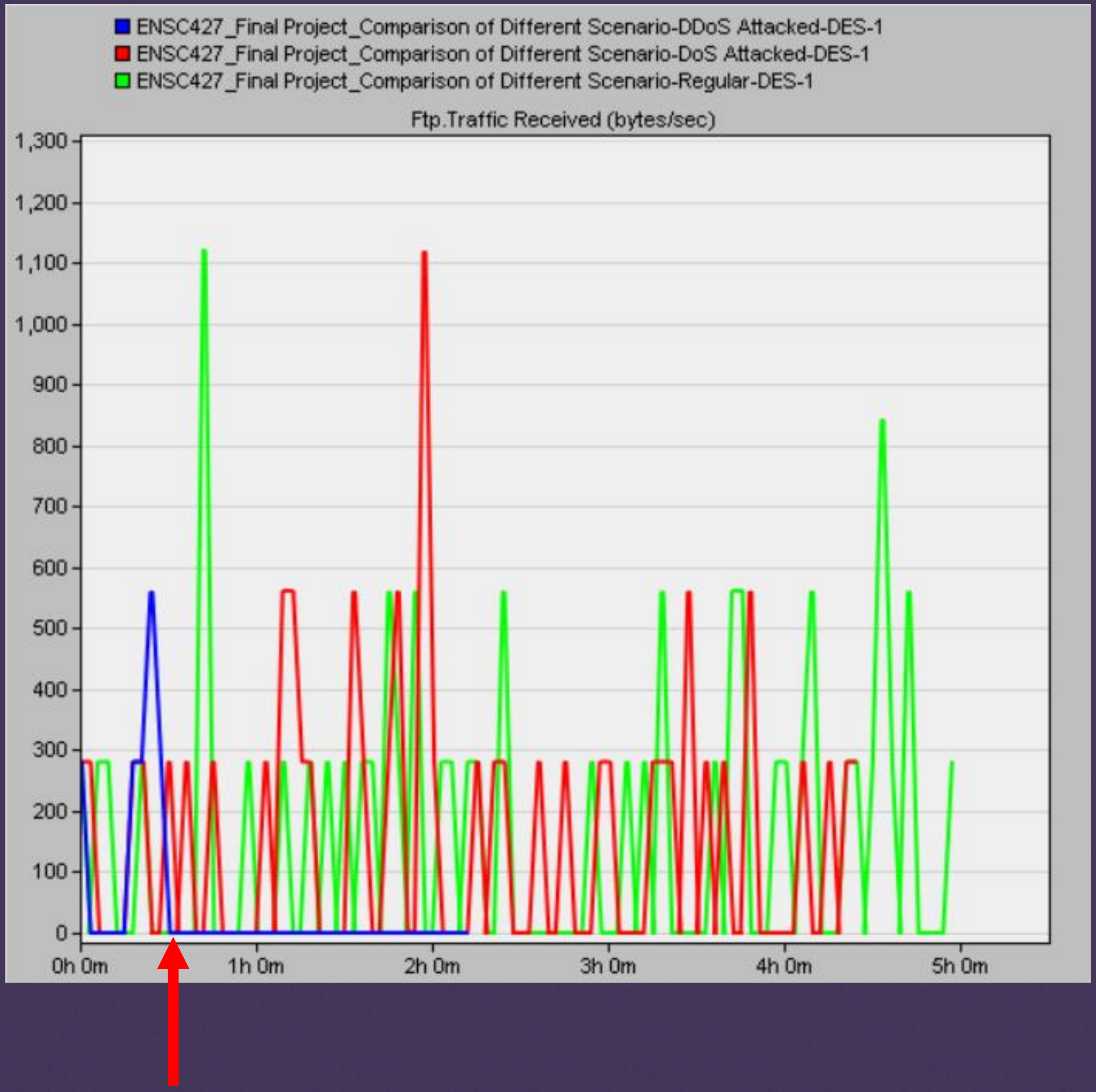


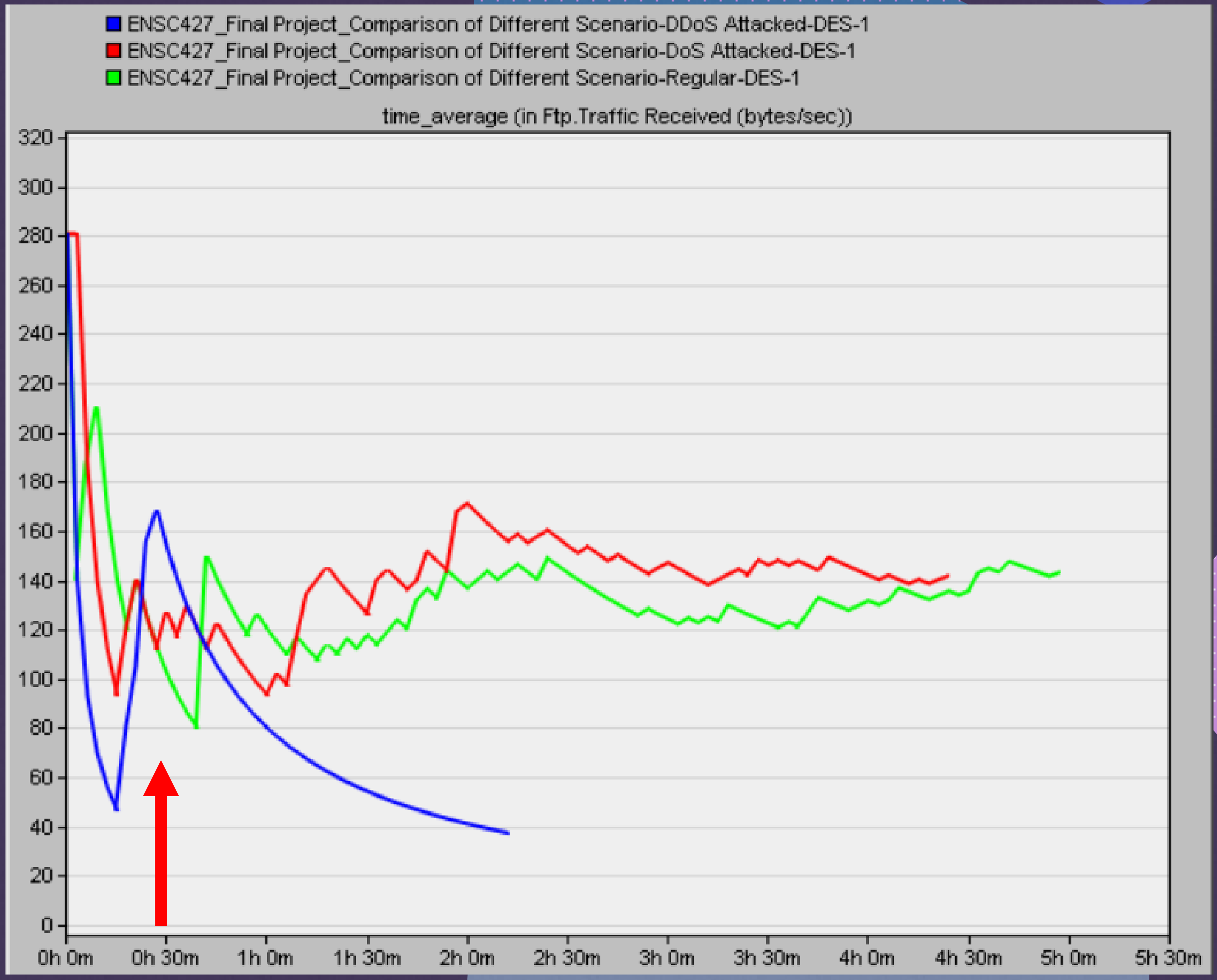
Simulation Results (DB Query Traffic Sent)



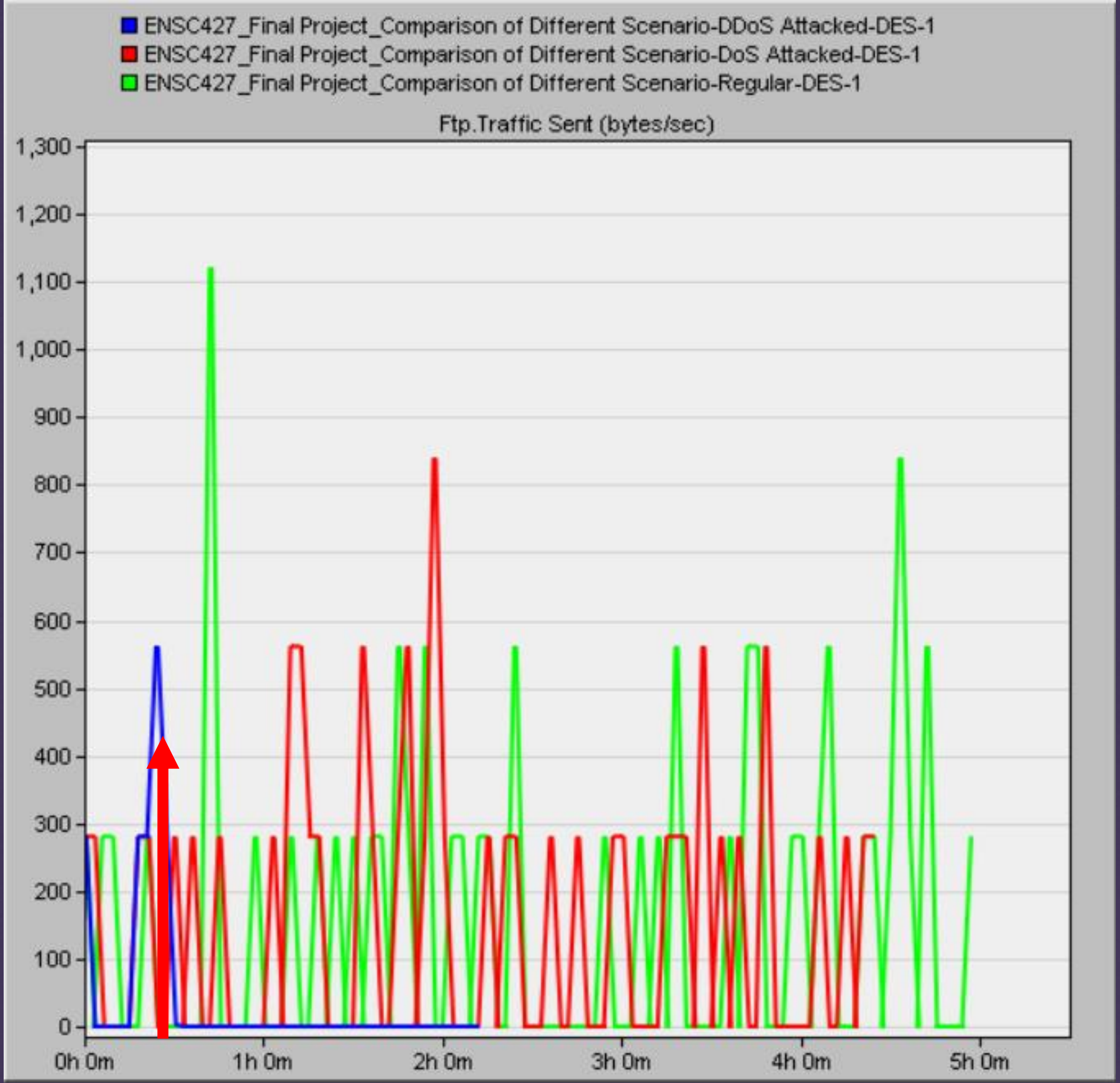


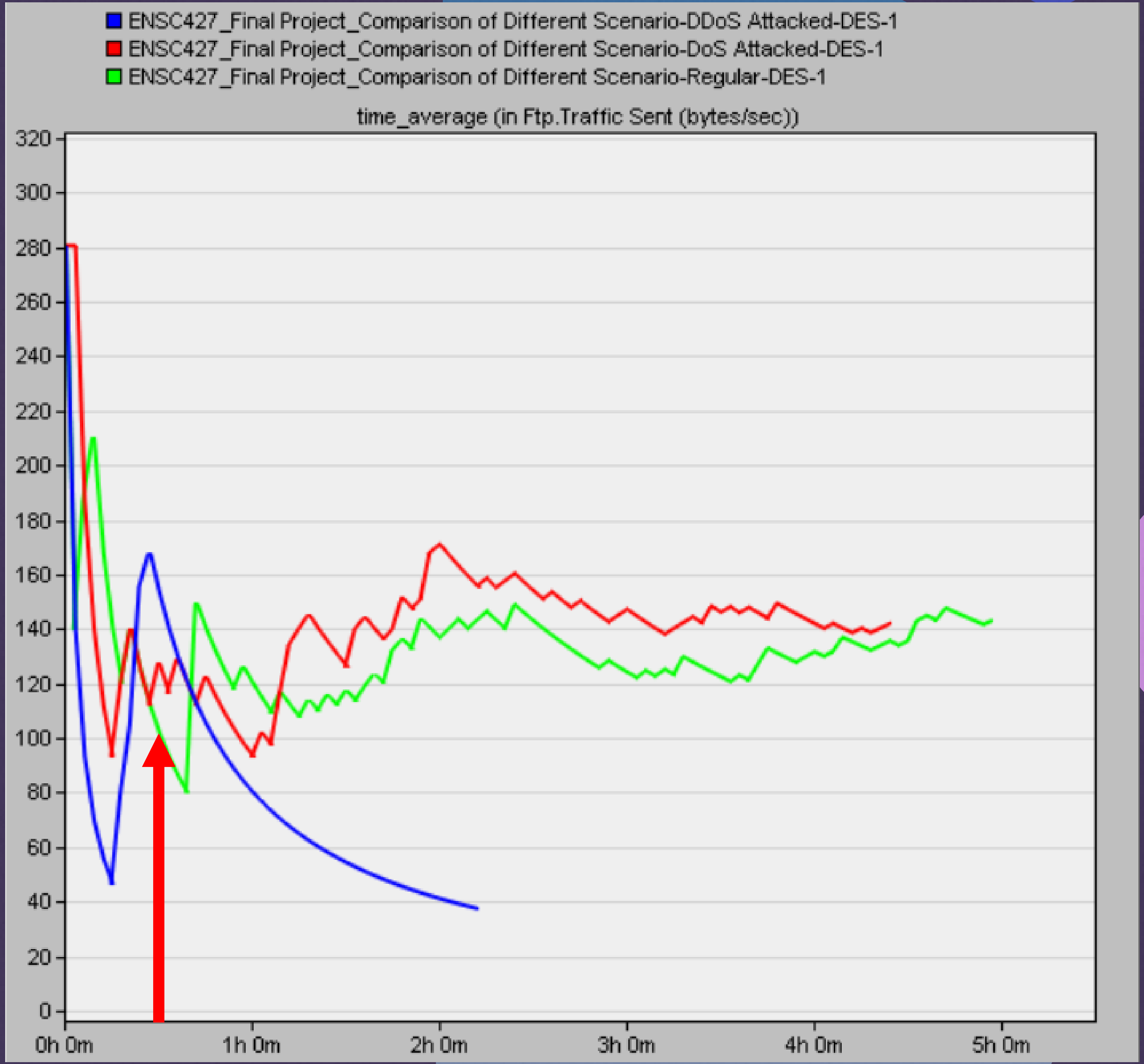
Simulation Results (FTP Traffic Received)





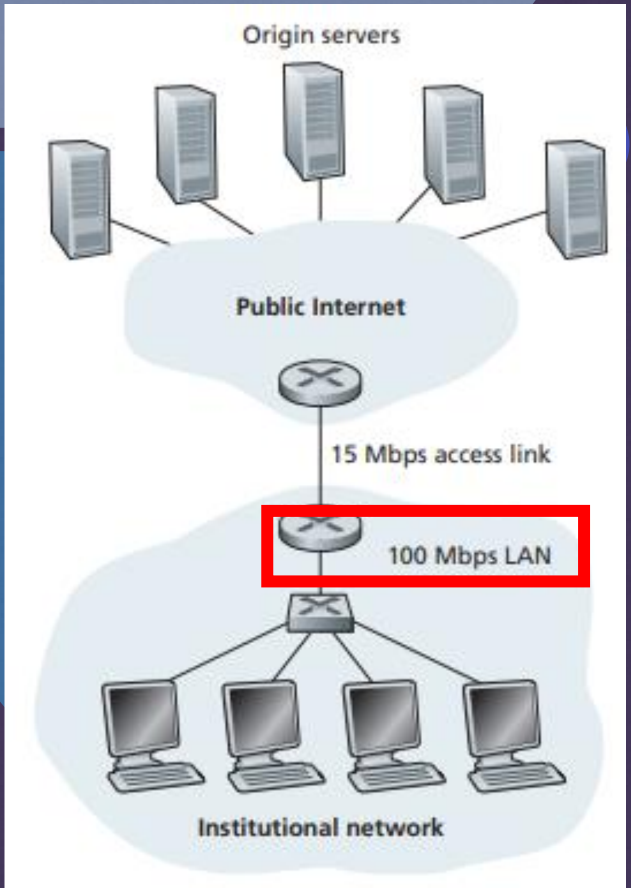
Simulation Results (FTP Traffic Sent)

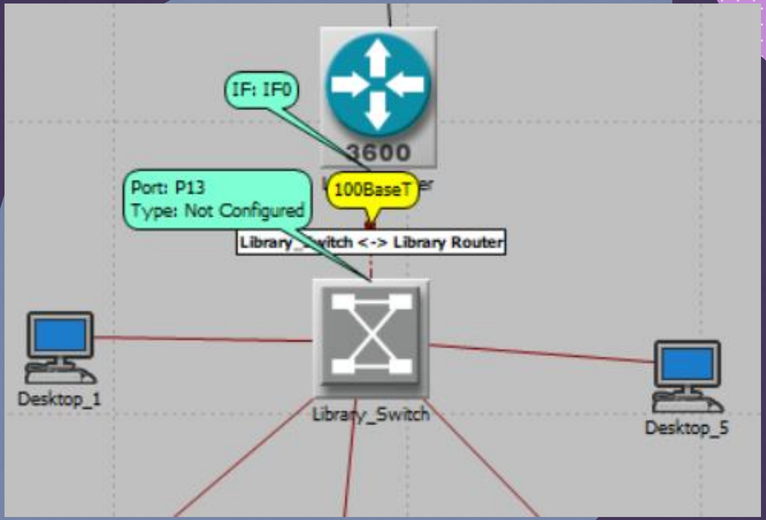




Discussion

- in the comparison between DoS and normal network topology, though there was decrease in response time, no big damage was inflicted.
- Our LAN used 100BaseT which is the predominant form of Fast Ethernet
- DDoS attack showed significant impact on the network service
- The limitation of DoS:
  - Since all traffic emanates from a single source, its prevention is easy





References

- “What is a distributed denial-of-service (ddos) attack ...” [Online]. Available: https://www.cloudflare.com/en-ca/learning/ddos/what-is-a-ddos-attack/. [Accessed: 27-Nov-2021].
- Webopedia. 2021. *What is a DDoS Attack? | DDoS Attack Meaning & Definition*. [online] Available at: <http://www.webopedia.com/TERM/D/DDoS_attack.html> [Accessed 27 November 2021].
- “DDoS: Detect and mitigate attacks with steelcentral NetProfiler,” *Riverbed Blog*, 09-Jan-2019. [Online]. Available: https://www.riverbed.com/blogs/ddos-detect-mitigate-attacks-steelcentral-netprofiler.html. [Accessed: 27-Nov-2021].
- “Ping of Death DoS Attack Simulated in Riverbed (OPNET) modeler” [Online]. Available: https://www.youtube.com/watch?v=cdxmx2wZ6HA [Accessed: 28-Nov-2021]
- “DDoS quick guide - CISA.” [Online]. Available: https://us-cert.cisa.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf. [Accessed: 27-Nov-2021].