Special Topic

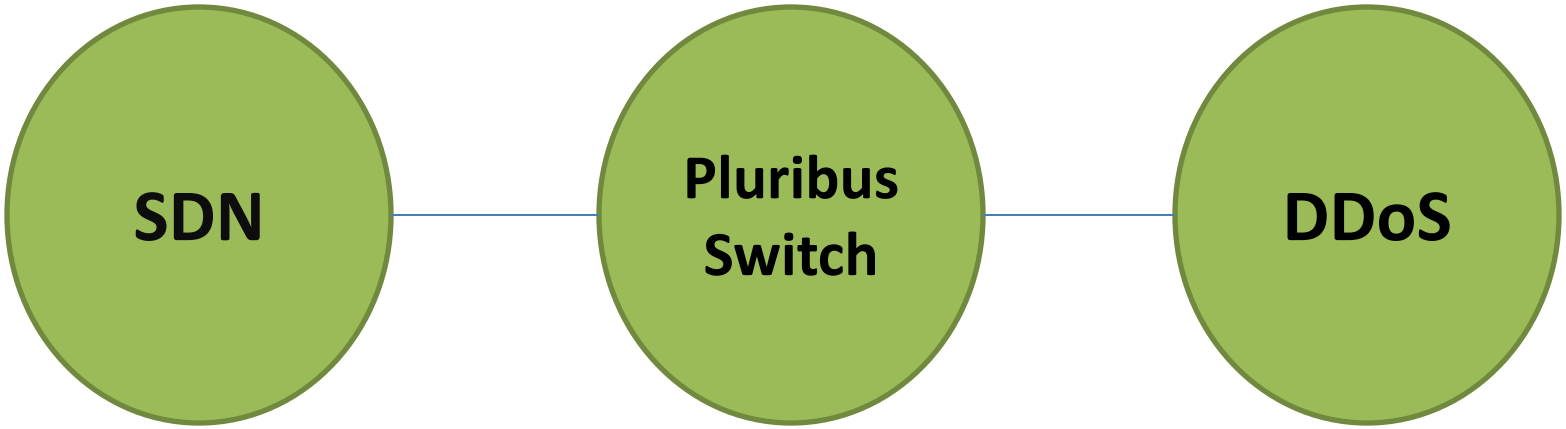
DDOS attack detection and prevention in Pluribus Switch

Guide: Prof. Malashree S

Contents

- Introduction
  - SDN
  - DDoS
  - Pluribus Switch
- Problem Statement
- Detection and Prevention technique
- Future Works
- References

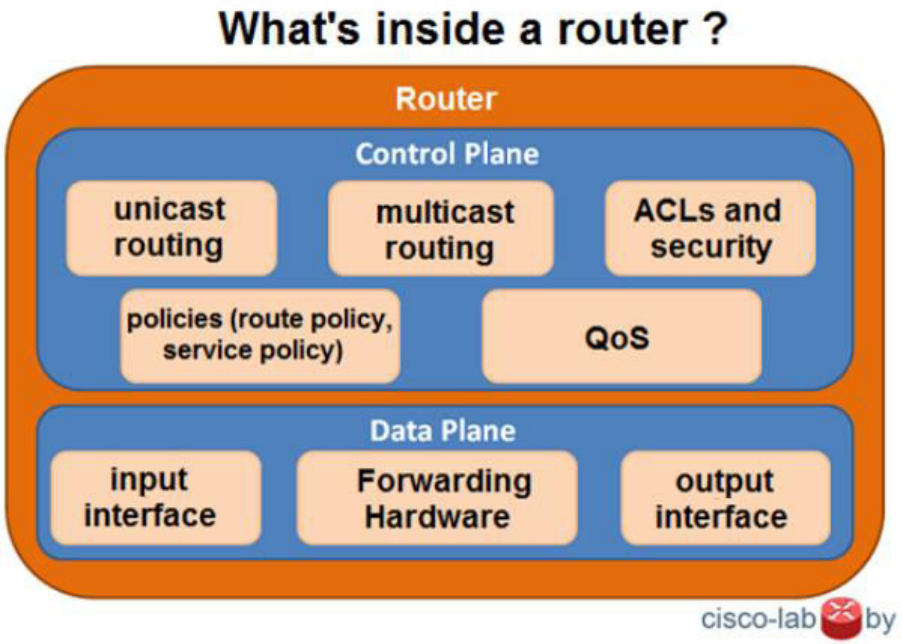
Introduction



Software Defined Networking (SDN)

Planes in Telecom Architecture

Data Plane → Control Plane → Management Plane



Control Plane

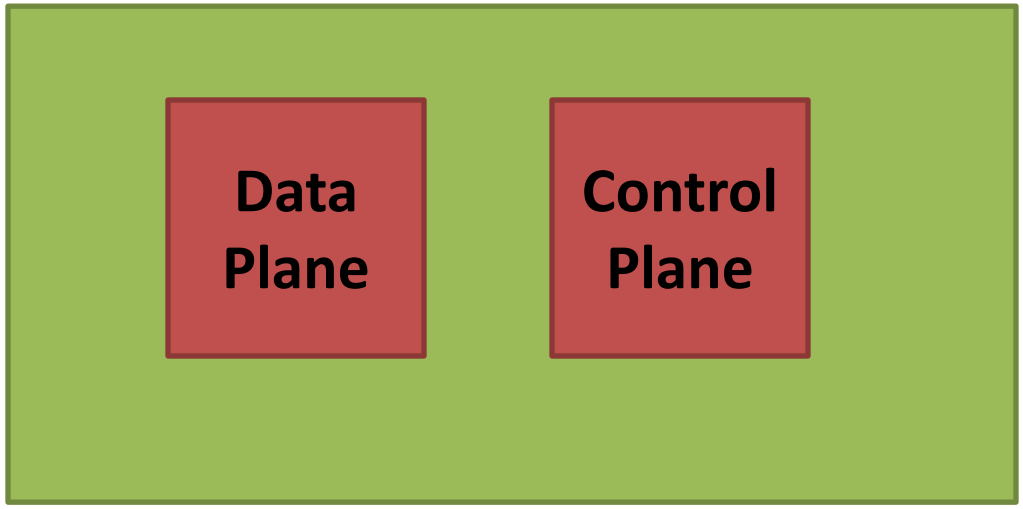
- The control plane is primarily about the learning of routes.
- **Control plane** is the part of the router architecture that is concerned with drawing the network map, or the information in a routing table that defines what to do with incoming packets.

Data Plane

- Actually moving the packets based on what we learned.
- The data plane (sometimes known as the user plane, forwarding plane, carrier plane or bearer plane) is the part of a network that carries user traffic.
- The data plane enables data transfer to and from clients, handling multiple conversations through multiple protocols, and manages conversations with remote peers.
- Data plane traffic travels through routers, rather than to or from them.

Software Defined Networking

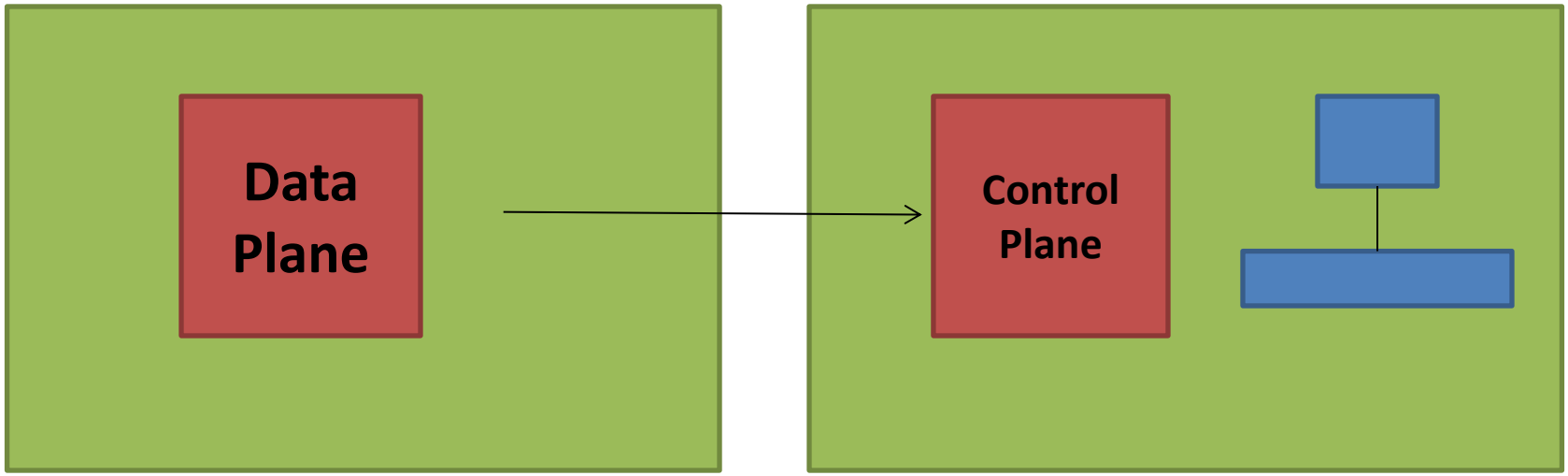
- In conventional networking, all three planes are implemented in the firmware of routers and switches.



Traditional Routers

Software Defined Networking cont..

- SDN decouples the data and control planes and implements the control plane in software instead, which enables programmatic access to make network administration much more flexible.



Router with SDN

Control plane implemented in computer software

Advantage of SDN

- Dynamic access and administration.
- A network administrator can shape traffic from a centralized control console without having to touch individual switches.
- The administrator can change any network switch's rules when necessary -- prioritizing, de-prioritizing or even blocking specific types of packets and IP and **thus prevent users from attacking network.**

Pluribus Switch

- A server switch by **Pluribus Networks** which employs SDN technology
- It has its own **Pluribus Netvisor Analytics Engine** which runs in it(OS), which allows user to view all the packet and other network related information.
- These switches have its own
  - Memory
  - RAM
  - Processor chip
  - Other components of Traditional switch

Pluribus Netvisor Analytics Engine

- With help of this following data will be available to users
  - Port information
  - Network topology
  - Traffic information
  - Individual packet data
  - Overall packets and their details

Pluribus Switch Command Line Interface

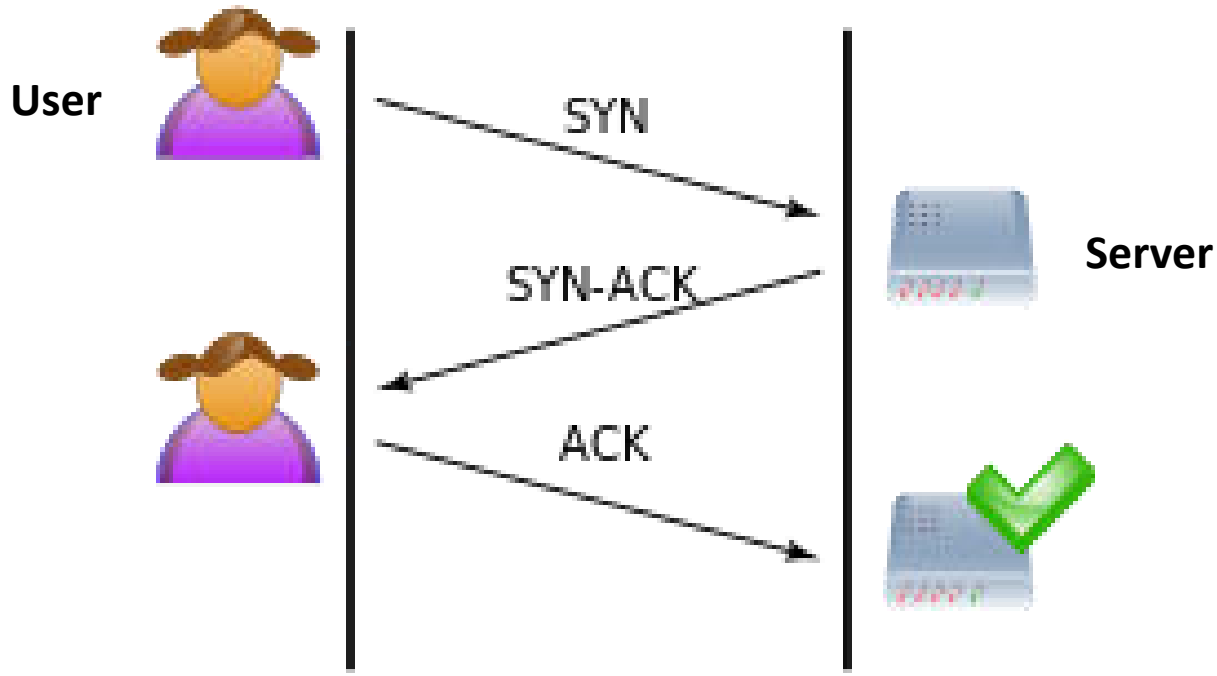
- The Netvisor Command Line Interface (CLI) provides powerful analytical commands to retrieve data from switch and all data is also available to Netvisor APIs.
- Examples
  - *'connection-show'*
    - display all connections across the fabric
  - *'client-server-stats-show'*
    - a summary per IP address
  - Vflow
    - to disable a communication

Distributed Denial of Service-DDoS

- In computing distributed **denial-of-service (DDoS) attack** is an attempt to make a machine or network resource unavailable to its intended users.
- Types
  - Internet Control Message Protocol (ICMP) flood
  - **SYN flood**
  - Teardrop attacks
  - Peer-to-peer attacks
  - Application-level floods
  - HTTP POST DDOS attack

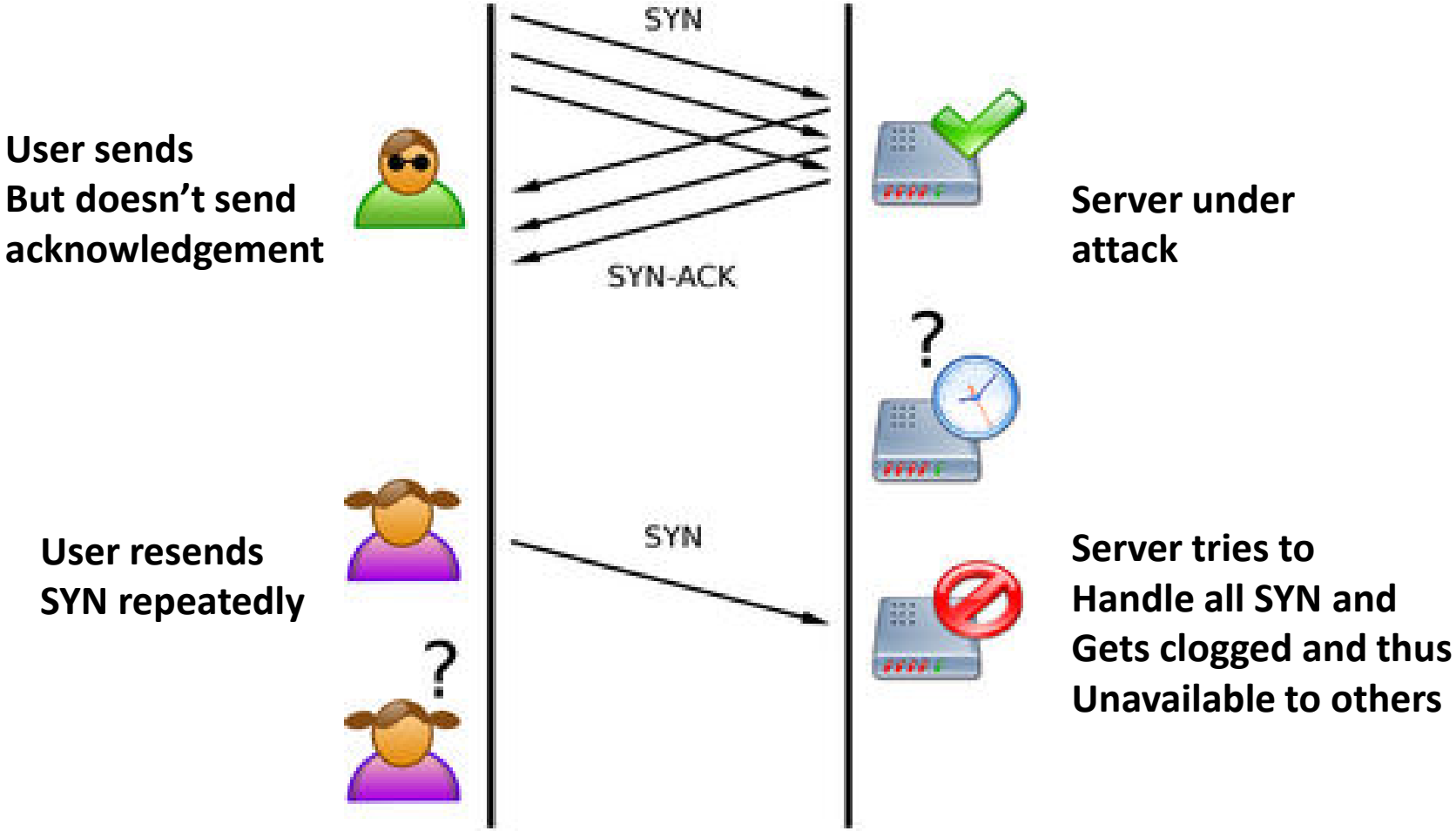
SYN flood

- Normal TCP 3-Way Hand shake



SYN flood cont..

- TCP connection during attack scenario



Problem Statement

- Lots of attack is happening in the world of networking in which **DDOS** is one of the prominent attack.
- This client to server attack which is happening using data packets, will have to pass through links and switches.
- Server switches are available from which traffic data can be retrieved
- This retrieved data can be analyzed at regular intervals and attacks can be predicted and actions might be taken for the same.

Technique Used

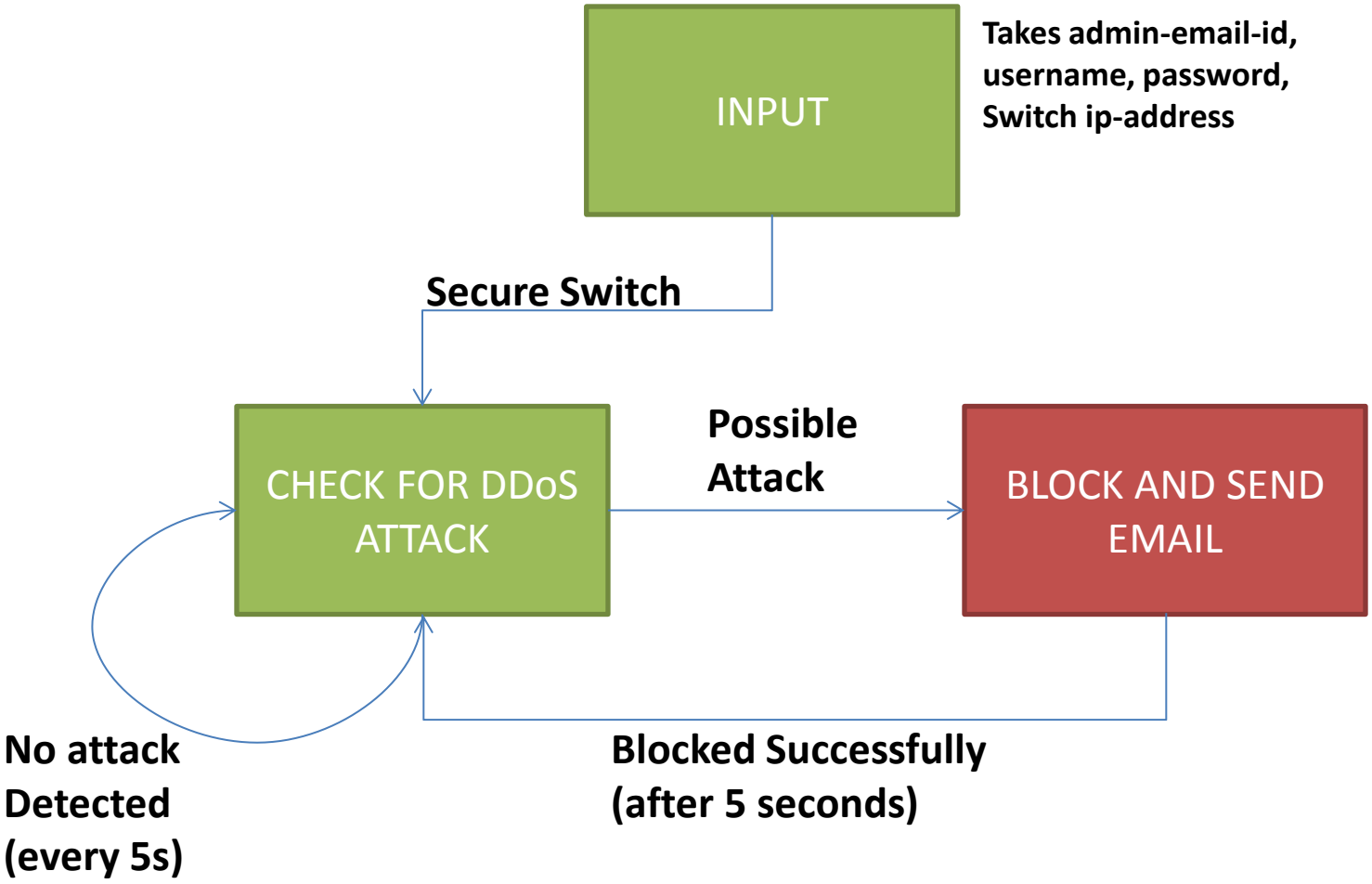
DDoS Detection technique

- The software does following at regular interval of 5 seconds
  - Connect to the switch
    - Using ssh, username and password
  - Retrieve data of packets for each client-server pair along with their SYN count
    - Run ‘client-server-stats-show’ command in the switch cli
  - Analyze the whole data retrieved to see all those tuples for which SYN count is greater than 1000 and return all those client-IP addresses
    - Input the data and scan and check for syn_count>1000

DDoS Prevention technique

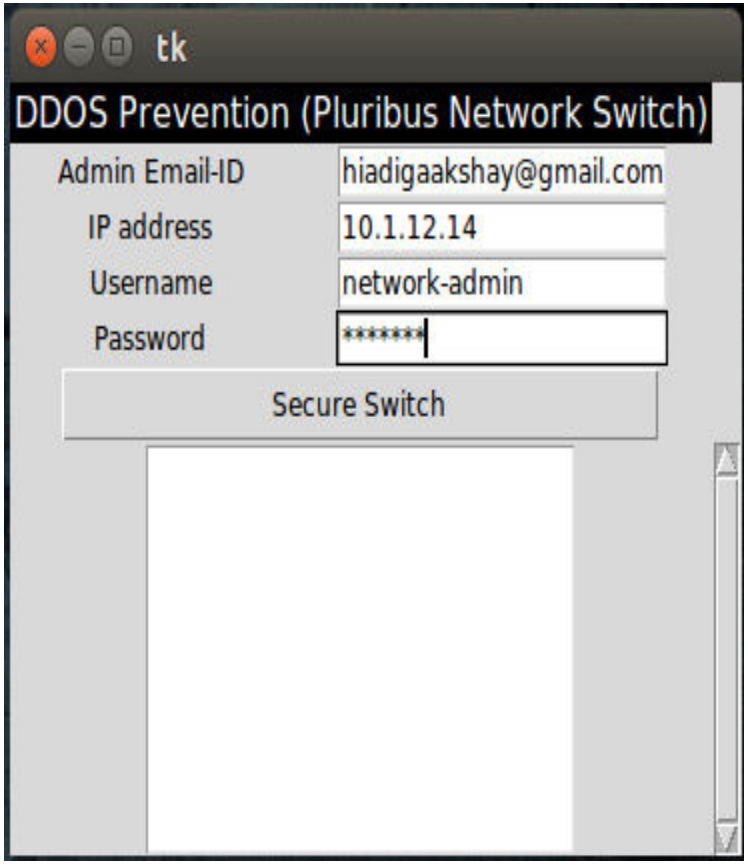
- The detection algorithm is run at every 5 seconds and it returns a set of IP addresses which try to do a SYN flood DDoS attack.
- For each of those IP addresses
  - The pluribus netvisor's 'vflow' command is used and IP's are blocked from communication thus preventing any further SYN flood happening
  - A e-mail is set to the switch admin regarding this, so that he can take any further action required.

Program Flow



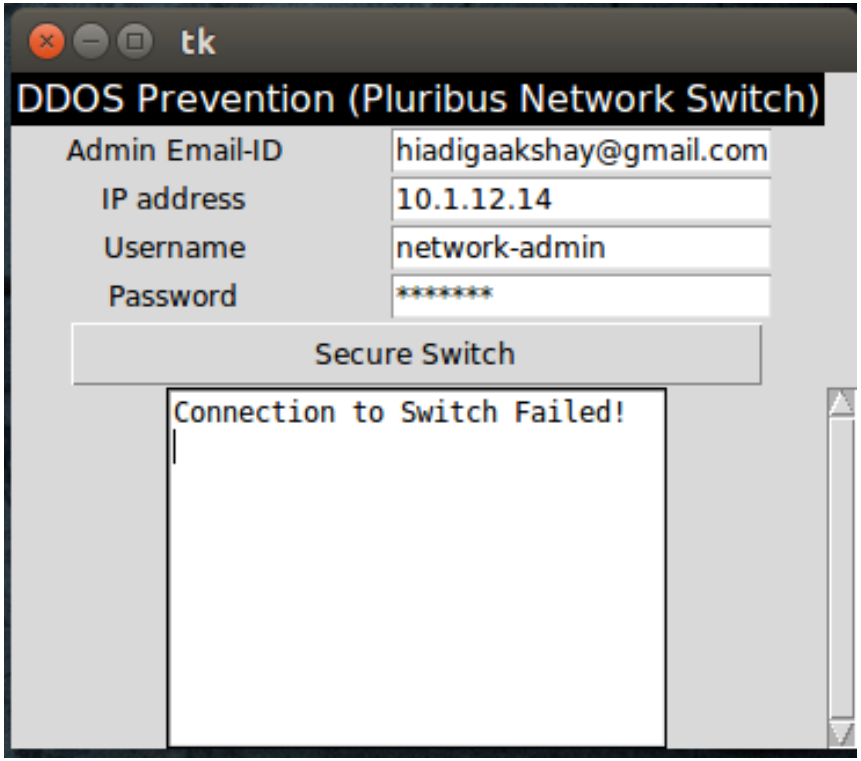
DEMO

- Initially it asks for
  - Admin Email-ID
  - Switch IP-address
  - Switch Username
  - Switch Password



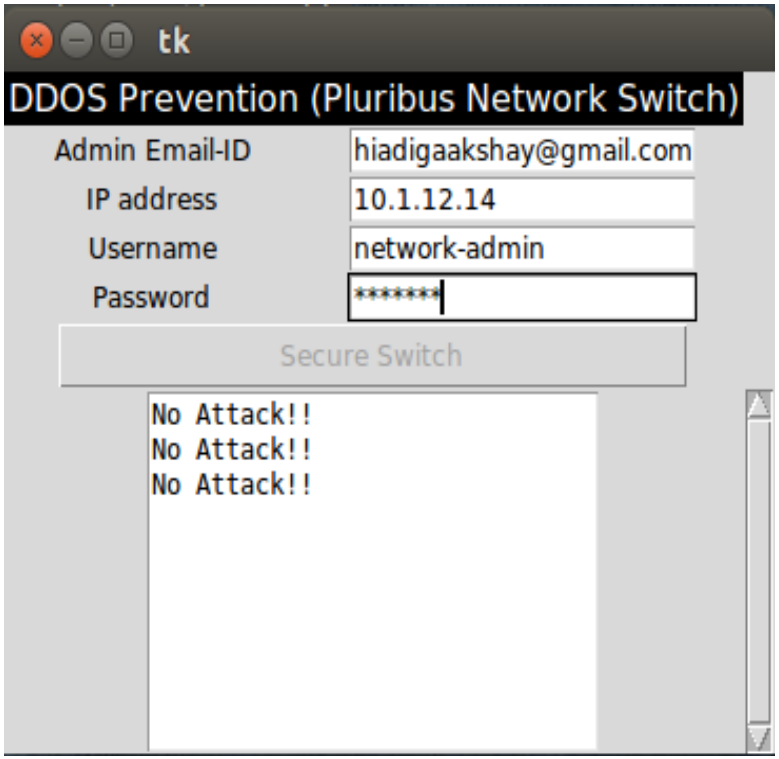
DEMO cont..

- On wrong username and password..



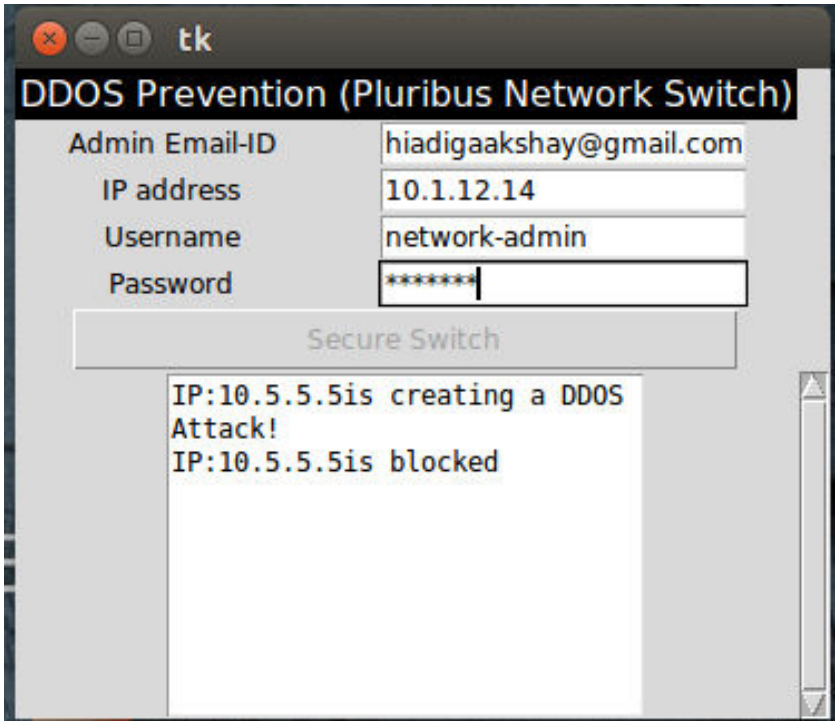
DEMO cont..

- After providing user data, the switch security can be started by clicking on '*Secure Switch*' button
- This will trigger a forever loop which will keep checking for attack and take action mentioned previously



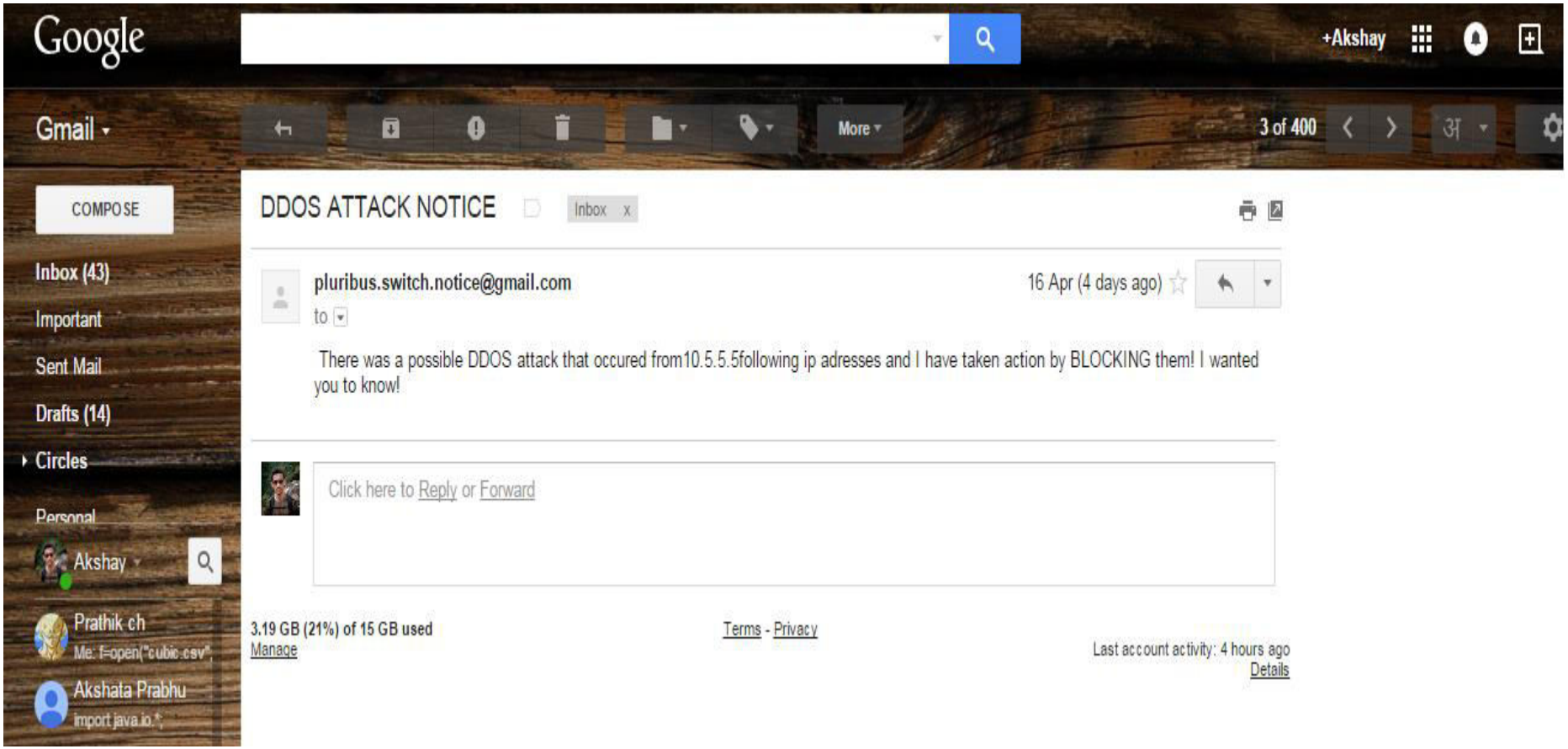
DEMO cont..

- When an attack is detected
  - The IP is first blocked



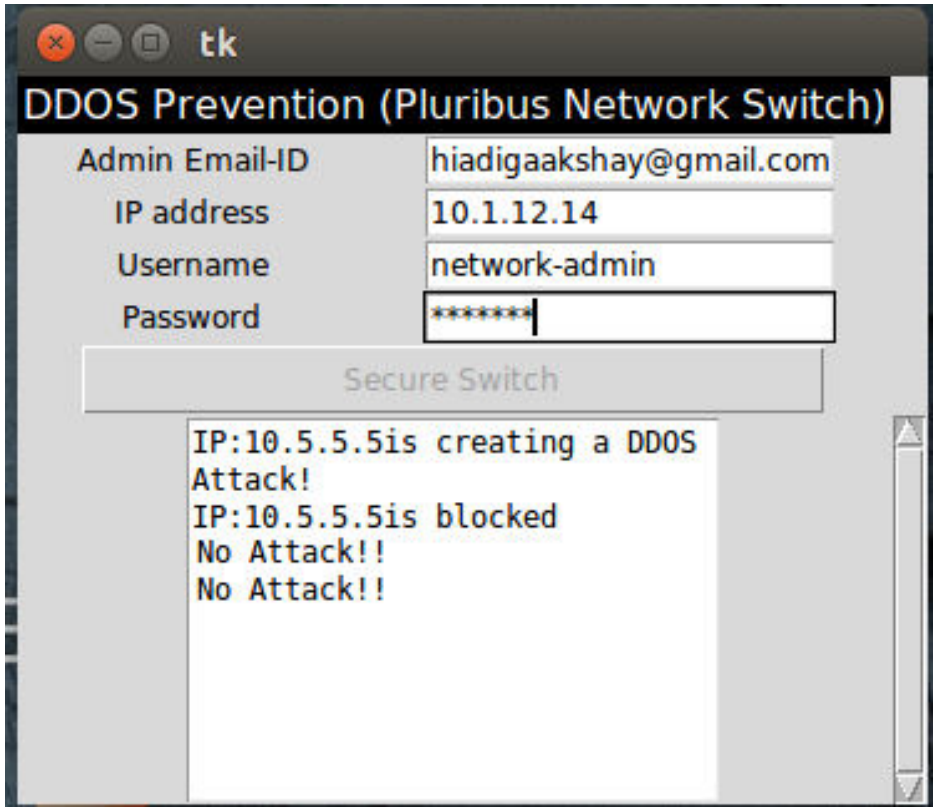
DEMO cont..

– A mail is sent to the Switch Admin regarding the same



DEMO cont..

- And the checking process continues forever..!



Future Works

- This can be further applied to detect ICMP flood scenarios which is one more type of DDoS attack.
- IP spoofing detection algorithm can be incorporated with this program thus able to detect users who try to create an attack by spoofing their IP.

References

- [1] Pluribus Switch Working and Basics - PN-WP-analytics-2-0.pdf
- [2] Command Line Interface for Pluribus Switch - pocket-guide-vflows-v22.pdf
- [3] how SYN flood happens in real - http://en.wikipedia.org/wiki/SYN_flood

Thank You Folks!