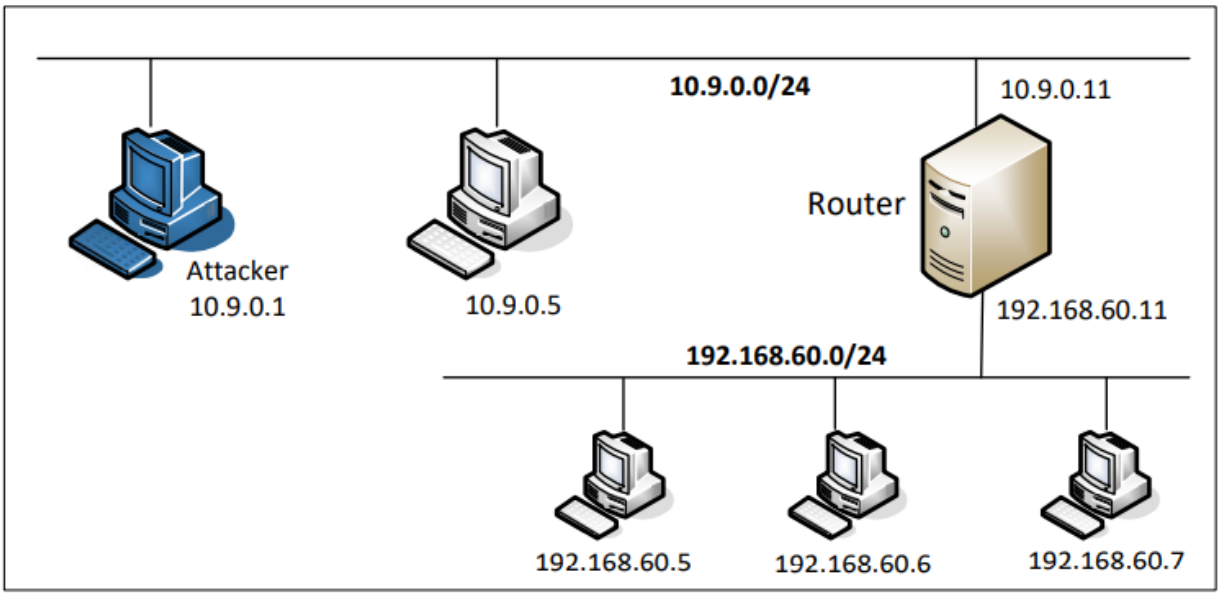
CSE - 406

Online on Firewall

A **SYN flood** is a form of denial-of-service attack (**DOS**) in which an attacker sends a succession of **SYN** requests to a target's system. This is a well known type of attack and works if a server allocates resources after receiving a **SYN**, but before it has received the **ACK**. This attack can be prevented by limiting the number of connections from a specific IP.

Now, we want to be extra cautious to prevent our internal network from such attacks. First of all, we want the hosts in the external network to communicate with the internal network servers through **telnet** connection only. Secondly, each IP address in the external network can make at most 3 connection requests and further request attempts will be dropped.

Now, you have to write down necessary firewall rules using ***netfilter*** to achieve this.



Hint: A **TCP** connection starts with a **SYN** packet i.e. a packet where the **SYN** flag is set in the **TCP** header.