COMP435 Written Assignment 5 Name: _____

Question 1: Packet Filters You are tasked with building a packet filter firewall. You are securing a small research lab subnet which can be addressed as `10.20.30.0/24`. A subnet is a logical subdivision of a network and we can use a subnet mask to identify the range of IP addresses that belong to a subnet.

The details of the scenario as follows:

- Public web server: 10.20.30.10 (HTTPS only; block HTTP).
- SSH into that web server is allowed only from the campus admin network 203.0.113.0/24.
- Clients in the lab may make outbound DNS queries (via TCP/UDP to port 53).
- Everything else should be denied.

1.1. Fill in the packet filter

Rule	**Dir**	**Src Addr**	**Dest Addr**	**Protocol**	**Dest Port**	**Action**
A	In	External	10.20.30.10	TCP	_____	Allow
B	In	203.0.113.0/24	10.20.30.10	_____	22	Allow
C	In	External	10.20.30.10	TCP	80	_____
D	Out	10.20.30.0/24	External	UDP	_____	Allow
E	Either	Any	Any	Any	Any	Deny

Table 1: Q1: Packet Filter (first match wins)

1.2. For each of the following test packets, indicate whether the packet would be allowed or denied by your packet filter.

#	**Direction**	**Src**	**Dest**	**Protocol**	**Dest Port**	**Allow / Deny**
1	In	198.51.100.9	10.20.30.10	TCP	443	_____
2	In	203.0.113.55	10.20.30.10	TCP	22	_____
3	In	198.51.100.7	10.20.30.10	TCP	80	_____
4	In	198.51.100.7	10.20.30.10	TCP	22	_____
5	Out	10.20.30.42	8.8.8.8	UDP	53	_____
6	Out	10.20.30.42	93.184.216.34	TCP	443	_____
7	Out	10.20.30.77	203.0.113.10	UDP	4000	_____
8	In	203.0.113.200	10.20.30.10	TCP	443	_____

Table 2: Q1 Test Packets

Question 2: Instrusion Detection Systems An organization installed a new intrusion detection system. On a typical day the organization's network will see 100,000 events, of which 10 are intrusions. The IDS will detect the 10 intrusions and will raise a total of 50 alarms. What is the alarm precision of the IDS? Show your work.

Question 3: The Network Stack 3.1. At what layer would you find IP addresses?

3.2. At what layer would you find MAC addresses?

Question 4: TCP 3-Way Handshake (Transport Layer) Why must TCP use a 3-way handshake instead of a 2-way handshake? What security or reliability properties does this provide?