Surname	:	Pendyala
Firstname	:	Praveen Kumar
Matrikel #	:	2919474

Group Members :
Shrikanth Diwakar (2492658)
Ankush Chikhale (2973449)

Problem 5.1

a. **Commoditization :**
   Commoditization means that how cloud services are treated as a commodity by the vendors and to provide cheap services in competitive environment how the paradigm shift is happening. Nec has mentioned that Initially in the beginning a central server was there, with the passage of time currently it is a switch that works in a L2/L3 Environment and for future they are predicting as a Bare Metal Switch.

b. **Why flow granularity in OpenFlow is said to be not predefined**
   Yes, it is true. There is nothing mentioned about any type of restriction in the flow granularity of the openflow. They give the flexibility to match any section of any type of supported match field is possible within this.

c. **Driver like abstraction on SDN Controllers**
   Lowest layer of SDN architecture has plugins or drivers that helps the controllers to interface with various networking devices .In previous data plane has layers that help them with abstraction and data plane has no such facility of abstractions present on them. The best example which provide this is the openflow protocol.

d. **Concept of “intents” in the context of Northbound Interfaces (NBIs)**
   In northbound API level of abstraction is unclear and also the scope is unclear. Thus the concept of intent comes into the role. Intent is what designed to include the conflict detection and its resolution in the design part only.

e. **Purpose of these two table**
   State table contains row entries as packet header fields and associated states per flow. Packet header fields are used as keys to query the table to fetch the associated state.

f. **Applicability of OpenState**
   Small protocols such as ARP, ICMP etc can benefit from OpenState. Traffic engineering, shaping and QoS can also benefit from OpenState.

g. **“port knocking” example is realized using OpenState**
State table contains the packet header fields which are matched to obtain the current state of port knocking. Once the current state is obtained, XFSM table is matched to see if the relevant event has occurred i.e. (if port number of the packet arrived matches the predefined port or not). If the event is determined to have occurred then corresponding action is taken else the state machine moves to default state again.

Problem 5.2

a. **State explosion and causes**
As More and more devices or services want to use the data plane then it is impossible to provide tunnelling to each and every route of the NFV and it will travel to all the services and no separate service chaining can be provided for the same.

b. **Path switching vs source routing**
Path switching eliminate the extra traffic and reduced it, as it does not allow traffic to pass through each and every switch. Source Routing vs Path Switching is compared by various parameters like MTU which Reduced, varies per path in source routing whereas Fixed, same as original in path switching. Virtualization Separate virtualization header whereas Built-in in path switching. Similiarly other parameters are compared for the same.

c. **Use a pointer field in Path switching and alternatives**
Path Header Pointer field points to the current label. Pointer field encodes start of current interface label & initialized to 0 and later Updated by each Path Switch by the length of its interface label.

d. **Case study 5 :**
One possible for blocking externally initiated connections would be checking for SYN flags in TCP connections. The firewall blocks all the TCP packets with SYN flag set and the direction of packet as external to internal network. This would require very less state information to be maintained at the firewall however a more complex setup could be monitoring the TCP sequence numbers as well. This also prevents the external packets that do not obey the TCP protocol initial SYN flag setting as well.

Also, to prevent state data accumulation at the firewall, the state can be cleared once the firewall sees a TCP connection close flag or use of timeouts or periodic cleanup of not recently used connections. This would be a necessary improvement on the existing setup for a more practical deployment.