1. **(5 points) Give one example of each a) SaaS, b) PaaS, and c) IaaS.  (Try to think of your own examples rather than the ones that are given in the book.)**

**Ans:**

a) SaaS: SaaS stands for Software-as-a-Service. SaaS provides the capabilities to the customer to use the provider’s application running on a Cloud infrastructure. The application running is accessible from various client devices through either a thin client interface.   
Example: Google Apps, Salesforce  
  
b) PaaS: PaaS stands for Platform-as-a-Service. PaaS provides capabilities to the customer to deploy onto the cloud infrastructure or acquired applications created using programming languages, libraries, services, and tools supported by the provider but does not manage or control the cloud infrastructure.   
Example: Heroku, OpenShift, Force.com  
  
c) IaaS: IaaS stands for Infrastructure-as-a-Service. IaaS provides the capabilities to the customer to provision processing, storage, network, and other fundamental computing resources where the customer is able to deploy and run arbitrary software, which even includes operating systems and applications but does not manage or control Cloud infrastructure.   
Example: Amazon EC2, Google Compute Engine, Rackspace

**2. (5 points) Explain what problem the HSMs solve and how exactly  an HSM helps with the security of outsourcing IT to the Cloud.**

**Ans:**

Hardware Security Modules (HSMs) are hardened, tamper-resistant hardware devices that strengthen encryption practices by generating keys, encrypting and decrypting data, and creating and verifying digital signatures. Some hardware security modules (HSMs) are certified at various FIPS 140-2 Levels. Hardware security modules (HSMs) are frequently used to:

1. Meet and exceed established and emerging regulatory standards for cybersecurity

2. Achieve higher levels of data security and trust

3. Maintain high service levels and business agility

HSM helps in keeping the integrity of outsourcing the IT infrastructure to the cloud. Even though external agents like amazon will be hosting and managing your IT infrastructure but they won't be having any access to any of the machines since they are binded with HSM (ex: RSA Key) which ensures that the information inside is intact.

**3. (10 points) Explain what it means that an instruction is not virtualizable and give an example of such an instruction’s behavior. Provide several examples of x86 instructions that are not virtualizable.**

**Ans:**

For instruction to be virtualizable, Popek and Goldberg requirement must be met, but in the case when the instruction is not virtualizable these requirements are overruled. The operating system runs in modes i.e. user mode or system mode. When any privileged or sensitive instruction which is supposed to run under only system mode and the instruction traps and when executed in user or guest mode. Any attempt of utilizing or modifying any system application or resource by the user is termed as not virtualizable instructions.   
  
Non-virtualizable instructions fall into three classes. In first-class, A major problem is that the processor has only one register for each of these, which means that they need to be replicated for each virtual machine. In the second class, the instructions that copy parts of the STATUS register into either general registers or memory and in third class, instructions that reference of the storage protection system, memory, or address relocation systems.   
The problem with x86 instructions is that the instructions were allowed while being executed in the user mode to transfer the value of the STATUS register to a general register. This instruction is behavior-sensitive in the Popek and Goldberg taxonomy because it allows a user program to discover which mode is running in it.

**4. (10 points) Explain how a hypervisor can be run on top of a hypervisor and provide an example where such a feature is being used.  Can KVM run on top of XEN?**

**Ans:**

Hypervisors can easily be run on top of another hypervisor. I can explain the entire thing by taking an example. Let's consider this system Dell Precision 7920. It has dual sockets on the motherboard and can accompany 2 intel Xeon 8280L processors. This gives us a sufficient number of cores (28 \* 2) and 2.7 GHz per core. The motherboard has 24 slots wherein we can put 24 sticks of DDR4 memory. Above such hardware, we can run VMware ESX flawlessly and create virtual machines and run our chosen operating system  (windows in my example). Inside the virtual machine, we can then install a type 2 hypervisor like VM Ware workstation pro or Oracle Virtual box and create another virtual machine inside the primary virtual machine. This explains completely how a hypervisor can be run on top of another hypervisor. Specifically, we can run type 2 hypervisor over type 1 hypervisor.

No, KVM can not run on top of a  XEN hypervisor.

KVM is built into Linux as an added functionality. It lets you convert the Linux kernel into a hypervisor. It is sometimes confused with a type 2 hypervisor (see definition below). It has direct access to hardware along with virtual machines it hosts. KVM is an open-source hypervisor that contains all the features of Linux with the addition of many other functionalities.

**5. (10 points) Explain the problem that the I/O MMU solves. What problems are introduced when using the I/O MMU?**

**Ans:**

Input-Output Memory Management Unit (I/O MMU) maps the device visible virtual address to a physical address by connecting a Direct Memory Access (DMA) to the main memory.

The problems introduce when using I/O MMU are:   
1. Direct Memory Access additional safety performance issues as it enables an I/O device to read and write-host RAM directly without involving the CPU.   
2. Security checks or encrypting disks, writes can incur by modifying I/O requests.

**6. (10 points) Explain how XEN supports I/O processing in a guest operating systems.**

**Ans:**

XEN support both paravirtualized and fully virtualized guests, respectively called PV and HVM. For guests running in HVM, XEN emulates low-level hardware and firmware components—such as graphic, network, and BIOS adapters, using techniques described in the previous section. Predictably, emulation often results in degraded performance. XEN deals with this by creating yet another mode, called PV-on-HVM (or PVHVM), in which an HVM guest is paravirtualized only partly. Xen's approach to handling physical I/O devices is straightforward and elegant. XEN creates a special environment—called a domain — for each guest.

**7. (10 points) What is the difference between the virtual machine and a container? Provide an example of a situation where you would use a Linux container rather than a virtual machine.**

**Ans:**

Differences between Virtual Machine and Container:  
1. Virtual Machines are used to run only a single application in an operating system, but the Container is used to run many applications.   
2. The resources (like memory, disk space, and CPU utilization) available in Virtual Machine are much lesser in size as compared to Containers.   
3. Containers have more economical ways than Virtual Machines to move to the cloud.   
4. Containers are more efficient than Virtual Machines as it provides more and necessary resources for any computation or processing.   
5. Virtual Machines can run more user or guest operating system and operating system have full control of the machine, whereas Contains have control of operating system userspace.   
  
Situations to use Container rather than a Virtual Machine   
1. While rewriting an application based on microservices, the user must use Container.   
2. Containers should not be used while writing any application from scratch.

**8. (10 points) NAT prevents the internal IP addresses from being seen outside. Can an ISP assign to a host behind a NAT box an IP address that is already assigned to some other host, which is not shielded by NAT)? If yes, explain why. If not, show what may be a problem with that.**

**Ans:**

No, an ISP cannot assign an IP address to a host behind a NAT box.  ISP can only assign an IP address to a NAT box.  It is the responsibility of the NAT box to anonymize the hosts present behind the NAT box. For each IP packet that goes outside, its source IP address is changed to  
the public IP address. Such address substitution is precisely a function of a NAT box. With  
that, a NAT box can assign the same public address to all packets that go through it. Hence,  
if a network has n entities, inside only one IP address—shared by all of them—it is used for  
external communications. Not only does this scheme allow the reuse of IP addresses, but it  
also anonymizes the network addresses behind the NAT box. For example, if the ISP is allowed to assign the IP address to the host behind the NAT box and they assign 172.217.12.164 ([www.google.com](http://www.google.com)) IP address to one of the hosts then all the hosts in the internal network of the NAT box who will be trying to reach google.com with its IP address will be directed to the host in the internal network and will return an error since google.com is not hosted on the host which has been misconfigured. The second problem associated will be that there won't be any anonymity, the ISP can know the details about the host. If it is a military base, which has some defense secrets in the host then it comes as a threat to national security as well since it can become prone to different kinds of attacks. If the ISP starts assigning individual IP addresses to hosts behind the NAT box (even if it becomes possible) then For IPv4, this pool is 32-bits (232) in size and contains 4,294,967,296 IPv4 addresses, it won't take much time and all the addresses will be over.

(Reference: Cloud Computing: Business Trends and Technologies, Pg. 164)

**9. (10 points) Given the implementation of a NAT box that we discussed in class, what is the major factor (independent on the memory capabilities) that limits the number of the active connections that a single NAT box can support at any given time? (In other words, consider the UDP packet header below and provide the absolute upper bound for the number of all possible UDP-based “connections.” (You don’t need to be concerned with the number of reserved ports.)**

**Ans:**

Lacking reliability, UDP applications must be willing to accept some packet loss, reordering, errors or duplication. If using UDP, the end-user applications must provide any necessary handshaking such as real-time confirmation that the message has been received. Applications, such as TFTP, may add rudimentary reliability mechanisms into the application layer as needed. If an application requires a high degree of reliability, a protocol such as the Transmission Control Protocol may be used instead.

Most often, UDP applications do not employ reliability mechanisms and may even be hindered by them. Streaming media, real-time multiplayer games, and voice over IP (VoIP) are examples of applications that often use UDP. In these particular applications, loss of packets is not usually a fatal problem. In VoIP, for example, latency and jitter are the primary concerns. The use of TCP would cause jitter if any packets were lost as TCP does not provide subsequent data to the application while it is requesting the re-sending of the missing data.

In TCP a single source IP is limited to 65536 theoretical max to the same destination IP.  Since UDP is stateless communication between two devices uses port and sockets. If each system only has 1 IP address, then a 'normal system' would be limited to an absolute maximum of 65536 connections. UDP is affected by the same limits. When a UDP packet leaves a NAT firewall it has to hold that port and remote IP address open for a certain amount of time for return packets to make it through. Assuming that we can use every single port 65536 will be the maximum limit.

**10. (20 points) You are building your own cloud with two remote data centers, each of which runs an Ethernet LAN. The respective sets of LAN addresses in these centers are A, and B. The data centers are interconnected with the MPLS-supporting networks, and so each data center has its own MPLS switch capable of performing layer-2 switching function. Show  how you can implement the Layer-2 WAN supporting the combined range of addresses,  A U B.  (You need to describe the switch logic in deciding how to handle outbound and inbound frames based on the destination addresses and define the LSPs needed for the WAN operation.)**

**Ans:**

In my Cloud network, I will be using 2 Mpls switch to connect both the internal networks  
will be using **Bi-directional LSPs with downstream or upstream label assignment.**They can be connected to the external network using a NAT or router. This will work perfectly in my scenario.