1. We are provided with the following parameters.

i. Size of the bucket: b bytes
ii. Rate of the bucket: r bytes/sec
iii. Maximum output rate: M bytes/sec

Therefore, the maximum burst time (T) is given as.

$T = b / (M - r)$ seconds

2.
i. AWS Direct connect allows the business or a user to connect their internal network with the Direct connect using a standard ethernet cable. One end of the cable is connected to the business or users router and the other end is connected to the AWS Direct Connect router. It allows the business to access the public cloud services as well as the VPC.

Pricing for AWS Direct Connect.

Direct connect considers two billing parameters.

a. Port hour: It measures the time that a particular port is provisioned to the user for using the AWS services. Even if no data is passing through the port, the user will be getting charged per hour. There are two types of port connections the user can select and the pricing for both the port connection is different.

Dedicated Connection: It is a physical connection between the user network port and the AWS network port which is present in AWS Direct Connect Location. Users can create this connection with the help of the AWS Management Console or CLI. The user is charged as long as there is a physical connection between the ports. With this connection, the user can get a port speed of 1,10 or 100 Gbps.

Hosted Connection: It is a logical connection between the user port and the AWS Direct connect which is created with the help of AWS Direct Connect Delivery Partner. In order to establish a connection, the user must contact the partner. The user can get a port speed of 50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, and 10 Gbps.

b. Data transfer out: It refers to the amount of data that is going out from AWS Direct Connect to the destination machine. Users are charged per Gigabyte of data.

I own a company whose data center is located in Sapporo Japan. Therefore I will select Equinix TY2 which is located in Tokyo Japan to connect with the AWS Direct Connect Service.

Users can select either a dedicated connection or hosted connection. Pricing for both the connection is different. For my convenience, I will select a dedicated connection with 1Gbps Port speed and its will cost be $0.285/hour.

Now comes the data transfer out rate part.

Its rate per gigabyte of data is $0.0410.

Equinix TY2 guarantees a port speed of 1Gbps if I have selected the 1 Gbps option for a dedicated connection. Also, Equinix TY2 data centers are SOC 1 Type II, SOC 2 Type II, ISO 27001, PCI DSS, ISO 22301, FISC certified.

References:
https://aws.amazon.com/directconnect/pricing/

https://www.equinix.com/data-centers/asia-pacific-colocation/japan-colocation/tokyo-data-centers

ii.
As we know that a single a single dedicated connection can be partitioned into multiple interfaces to access public resources such as the objects stored in S3 using public ip space and private objects stored in private ip space. The main question is how?

According to the IEEE802.1q paper , it says that the ability to create VLAN- dependent filtering database entries allows a bridge to support multiple end station (which in our case public and private resources) with the same individual mac address residing on different VLANs and end stations with multiple interfaces, each using the dame mac address as long as not more than one end station or interface that uses a given mac address resides in a given LAN.

Within a given network, there may be a combination of configuration requirements, so that individual Bridges may be called on to share learned information, or not share it, according to the requirements of particular VLANs or groups of VLANs. The Filtering Database structure that is defined in this standard allows both Shared and Independent VLAN Learning to be implemented within the same Bridge; i.e., allows learned information to be shared between those VLANs for which Shared VLAN Learning is necessary, while also allowing learned information not to be shared between those VLANs for which Independent VLAN Learning is necessary.

With this, we can partition dedicated connection into multiple virtual interfaces.

Resources:
http://magrawal.myweb.usf.edu/dcom/Ch3_802.1Q-2005.pdf

3.
We will make use of private interface to connect our AWS Direct Interface with the Virtual Private Cloud (VPC). Prerequisite before creating the interface make sure that the Virtual Private Gateway is installed in each VPC or a single Direct Connect Gateway is installed and it is connected to all the VPCs which needs to be access.
Here are the steps to connect our AWS Direct Connect with the VPC.

a. Search the AWS Direct Connect from the AWS Managemenet console and open it.

b. Choose Virtual interfaces and select create virtual interfaces.
c. SInce we have to connect our Direct Connect with our VPC, we will select create private interface option.
d. Under Virtual Private interface we have to insert the following parameters.
    i. Entering a name for private interface.
    ii. Selecting the AWS Direct connection that we want to use for the interface.
    iii. Now, we can select either Virtual Private Gateway or Direct Connect Gateway.
    iv. Next, it will ask for virtual interface owner, select another AWS account option and select the respective AWS account.
    v. After that, select the respective virtual private gateway. Each private interface will have only one virtual private gateway associated.
    vi. Select VLAN id, enter the id number for our Virtual Local Area Network(VLAN).
    vii. Next, we have to enter our BGP ASN number of our on premise peer router.
e. At the end, select create virtual interface button and then we are good to go.

Resources:
https://aws.amazon.com/directconnect/faqs/#:~:text=AWS%20Direct%20Connect%20requires%20Border,the%20connection%2C%20you%20will%20need%3A&text=A%20public%20or%20private%20ASN,ASN%2C%20you%20must%20own%20it.

4.
a.
NAT gateway is an AWS service that allows the business to connect their instances that are present within the private subnets in Amazon Virtual Private Cloud (VPCs) to the internet. Also, the resources which are present on the internet cannot initiate a connection with the instances which are present within the private subnets in VPCs. NAT gateways are installed in the public subnets because they can send the outbound traffic to the internet whereas the private subnet can't.

One of the advantages of NAT gateway is that it allows business to connect their network with the internet. The best case where we can use NAT is the multi-tier website where the web servers are present in the public subnets and the database which holds the sensitive data of the user is present in the private subnet. By setting up the configuration, security, and routing policies the web server can communicate with the database server. If the private subnets need to access the internet they can access it via NAT gateway which is installed in the public subnet.

The only disadvantage of using NAT is that the private subnet can't send the outbound packets directly over the internet. In order to send the packets over the internet, they have to use the NAT gateway present in the public subnet.

Resources:
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html

b.

Here is the thing. There are a total of 2 raised to 16 i.e. 65536 ports in the single NAT box. Also, there is a bit of confusion between the people that one port can have only one connection which is wrong.

A single listening port can accept more than one connection simultaneously.

TCP/IP packet has four fields for the addressing. Source address, Source port, a destination address, and destination port. If one client is having many connections to one of the same ports of the destination address then among the four fields only the source port would differentiate for different connections. As we know that port numbers are 16 bits long therefore the maximum no of connections any client can have to any given port will be 64k.

Also, multiple clients can each have up to 64k connections to some server's port.

So, its real limit is decided with the help of file descriptors. For each individual socket connection a file descriptor is given, so the limit is actually how many file descriptors the system is been configured to allow and resource to handle. The maximum limit is typically up to over 300k.

Resources:

https://stackoverflow.com/questions/2332741/what-is-the-theoretical-maximum-number-of-open-tcp-connections-that-a-modern-lin

https://serverfault.com/questions/541699/nat-gateway-maximum-connection-limit

5.
a.
Amazon Direct Connect and VPC are both the autonomous systems meaning they are not present in the same network. In order to establish a communication between the two external network system, an external routing protocol needs to be used. BGP (Border gateway protocol) is an external routing protocol which is used to exchange routing informations among the autonomous systems which are present on the internet. BGP runs on port 179.

b.
Yes, we can make use of our own ASN to connect to VPC. We can create public and private interfaces in AWS Direct Connect to access VPC. To create interfaces we need Autonomous System Number (ASN). We can use a public ASN or private ASN. Public ASN are used by the system if they want to exchange the information over the internet. Private ASN doesn't allow to exchange information over the internet. If we don't have an ASN, we can select from 64512 to 65534

c.
Regional Internet Registry is an organisation that handles the registration and allocation of internet number resources within a region of the world.The resources includes the

Autonomous system numbers and the IP addresses. There are five regional registries in the world which are African Network Coordination Centre (AFNIC), Asia-Pacific Network Information Centre (APNIC), American Registry for Internet Numbers (ARIN), Latin American and Caribbean Internet Addresses Registry (LACNIC) and Reseaux IP Europeens Network Coordination Centre (RIPE NCC). Since our data center is located in Sapporo Japan, we will make use of Asia-Pacific Network Information Centre (APNIC).

d. BGP (Border Gateway Protocol) is the external routing protocol which is used to communicate between the autonomous system. BGP contains all the routing information to the destination machine. Although, BGP is the most used protocol for inter domain activities, there are few vulnerabilities which are present.

i. Since BGP advertises their routing information to all the other external routers, there is a possibility of malicious device sending unwanted traffic to our network and resulting in Denial of Service Attack (DoS). This problem can be solved with the help of BGP - AS Validation. This feature helps network administrator from carelessly advertising network routes they do not control. It uses a Resource Public Key Infrastructure server to authenticate the several BGP prefixes originated from an expected autonomous system before the prefixes are allowed to be advertised.

ii. Each router maintains a table named routing table which contains all the routing information about the destination. Sometimes there is a possibility that certain BGP routes are missing from the routing table. If they are missing then check if the peering has been successful and check for the existence of route filters.

Resources:

https://arxiv.org/pdf/0907.4815.pdf

6.

It is given that the distance between the data center is 5.5 km and the speed of two dogs is 18km/hr. Therefore, time taken to travel from one data center to other is

Time = Distance / Speed

Therefore, TIme = 5.5 / 18 = 1100s

St Bernards Dog carry 3 disk of 7Gb each. Therefore total data = 3 * 7 = 21GB

Now ,

Data Rate = Data / Time

= 21000 * 8 / 1100 (Multiplied by 8 because 1 byte = 8 bits and we want the rate in bits)

= 152.73 Mbps

St Bernards dog provides the same services as renting the pipes for free.