**HOMEWORK – 3**

1)

Given:

* Total bucket size = b
* Token rate = r
* Max. output rate = M

To find: max. burst time(T)

* Token added to the bucket per second = 1/r
* Max. no. of token bucket can hold at any instance= b
* Since, M is max output rate and r is token rate, max burst time(T) will be:

**T = b/(M-r)**

*Sources: Textbook, Wikipedia (* [*https://en.wikipedia.org/wiki/Token\_bucket*](https://en.wikipedia.org/wiki/Token_bucket) *)*

2) a) *Business:*

If I own a company with data center in Sapporo, Japan, my preference for partner company to help connect this location to AWS service will be **Equinix, Inc.** The stepsthat I took to reach this conclusion are as follows:

i) I looked up the list of AWS Direct Connect locations which are found in many cities around the world to help connect a company’s local data center to AWS services using direct connect( a dedicated connection serving to link a particular client organization to AWS – instead of using the internet). We find that at : <https://aws.amazon.com/directconnect/locations/> . Here we see that there 3 Direct connect locations in Japan: (a) Equinix OS1, Osaka, (b) Equinix TY2, Tokyo and (c) AT Tokyo CC1 Chuo Data Center, Tokyo. We will prefer to connect to one of the 2 locations in Tokyo as it is closest to Sapporo – and hence will have least overhead.

ii) Next, I looked up the list of AWS direct connect delivery partners at the AWS documentation site: <https://aws.amazon.com/directconnect/partners/> . Here we go to Asia -> Asia-Pacific(Tokyo). We get a list of companies with details of their service.

iii) Next, we check out this list of companies. We find that Equinix, Inc has both: (a) support for dedicated connection (1 Gbps to 10 Gbps), (b) is approved for Hosted Connections of capacities from 50 Mbps to 10 Gbps – from Equinix TY2, Tokyo.

iv) We explore Equinix and AWS direct connect sites (listed in sources), to find the widespread option for high performance private access to AWS direct connect.

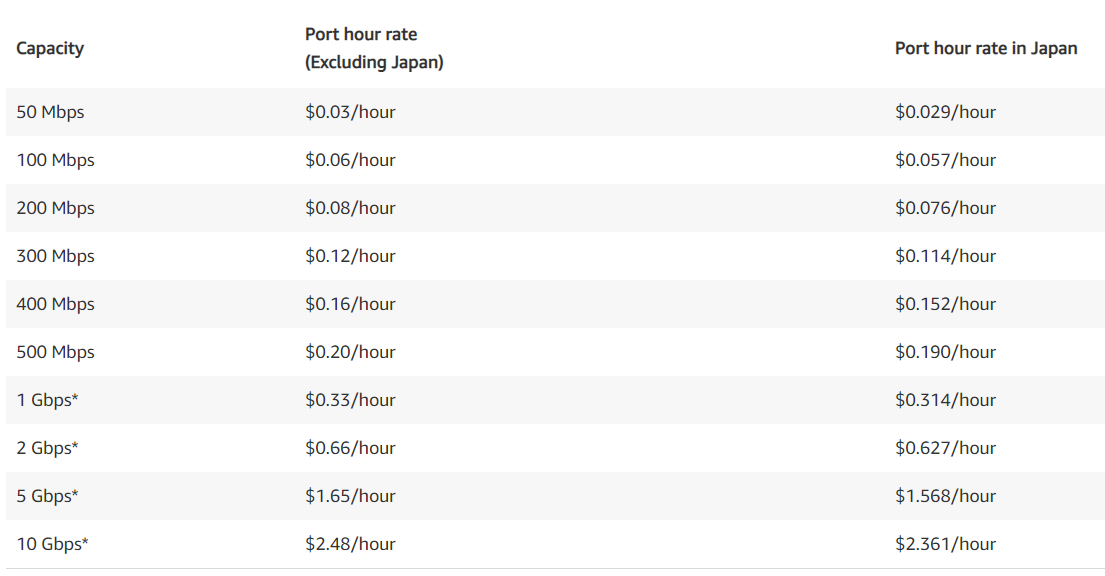
In conclusion, we note the following points to support choice for Equinix, inc:

* Offers many options for high-performance, private access to AWS Direct Connect.
* Provides latest technologies and the ability to migrate to hybrid computing.
* Equinix offers Amazon Direct Connect services over more geographical locations (200+) than any other provider.
* Supports dedicated connection from 1 Gbps to 10 Gbps, and hosted connection from 50Mbps onwards. This allows for great deal of flexibility.
* Provides cross connections either 1 or 10 Gigabits per second connections.
* Depending upon the demand, the AWS direct connect clients have a flexible range od data speed to choose from, enabling greater cost optimization.

**QoS guarantees:**

* **Security :** Equinix use advanced security equipment, techniques and procedures to control and monitor access to its International Business Exchange™ (IBX®) data centers. You typically pass through five security checkpoints that include 24/7 manned security stations, mantraps and biometric readers. Its low-profile building design allows a high level of security within the data center.
* **Reliability:** All equinix data centers are with back up systems, full UPS power and impressive an 99.9999% uptime.
* **Power** : Using full uninterruptible power supply (UPS) systems with N+1 redundancy levels or greater, backup generator systems and multicomponent temperature control system running 24/7, Equinix is able to provide efficient energy managements keeping costs down and providing maximum throughput.
* **Recovery :** Equinix Smart Hands offers 24-hour access to qualified technical support, helping to sustain and recover critical deployments.
* **Serves Most AWS markets:** Equinix provides direct connect services in 37+ business-rich AWS markets, which is more than any other provider.

**Pricing:**



*Sources: AWS Direct connection locations(* [*https://aws.amazon.com/directconnect/locations/*](https://aws.amazon.com/directconnect/locations/) *), AWS direct connect deliver partners(* [*https://aws.amazon.com/directconnect/partners/*](https://aws.amazon.com/directconnect/partners/) *), Equinix Fabric Portal – Ordering AWS Direct Connect (* [*https://www.youtube.com/watch?v=CixDJnubw-4*](https://www.youtube.com/watch?v=CixDJnubw-4) *), Equinix fabric – AWS Direct Connect (* [*https://docs.equinix.com/en-us/Content/Interconnection/Fabric/connections/Fabric-aws-direct-connect.htm*](https://docs.equinix.com/en-us/Content/Interconnection/Fabric/connections/Fabric-aws-direct-connect.htm) *), Equinix Partners AWS(* [*https://www.equinix.com/partners/aws*](https://www.equinix.com/partners/aws) *),* *Are Doing All You Can to Avoid IT Downtime? (* [*https://blog.equinix.com/blog/2019/07/02/are-doing-all-you-can-to-avoid-it-downtime/*](https://blog.equinix.com/blog/2019/07/02/are-doing-all-you-can-to-avoid-it-downtime/) *), AWS Direct Connect pricing(* [*https://aws.amazon.com/directconnect/pricing/*](https://aws.amazon.com/directconnect/pricing/) *)*

b) *Technical:*

AWS Direct connect can support hosted or dedicated connection from a corporation’s data center to AWS direct connect location. This can be provided by AWS partner networks(APNs) or the corporation can set up its own infrastructure.

The dedicated connection, that of 1 Gbps or 10 Gbps, can be partitioned into multiple logical connections by using industry standard 802.1QVLANs. Some of the partitions can be used to access the public resources like Amazon Simple Storage Service(S3) using a public IP address space while other partitions of the same connection can be used to access private resources like AWS EC2 instances running within VPC using private IP space. This arrangement ensures healthy network separation between private and public spaces.

Alternatively, we can create two systems: firstly, we attach a virtual private cloud(VPC) to the data center using virtual private gateway(VPG) to access services like EC2 instances, and secondly, we set up an additional public subnet to connect to other AWS services that do not run within the VPC, such as S3 storage buckets, Simple Queue Service( SQS) or Simple Notification Service (SNS).

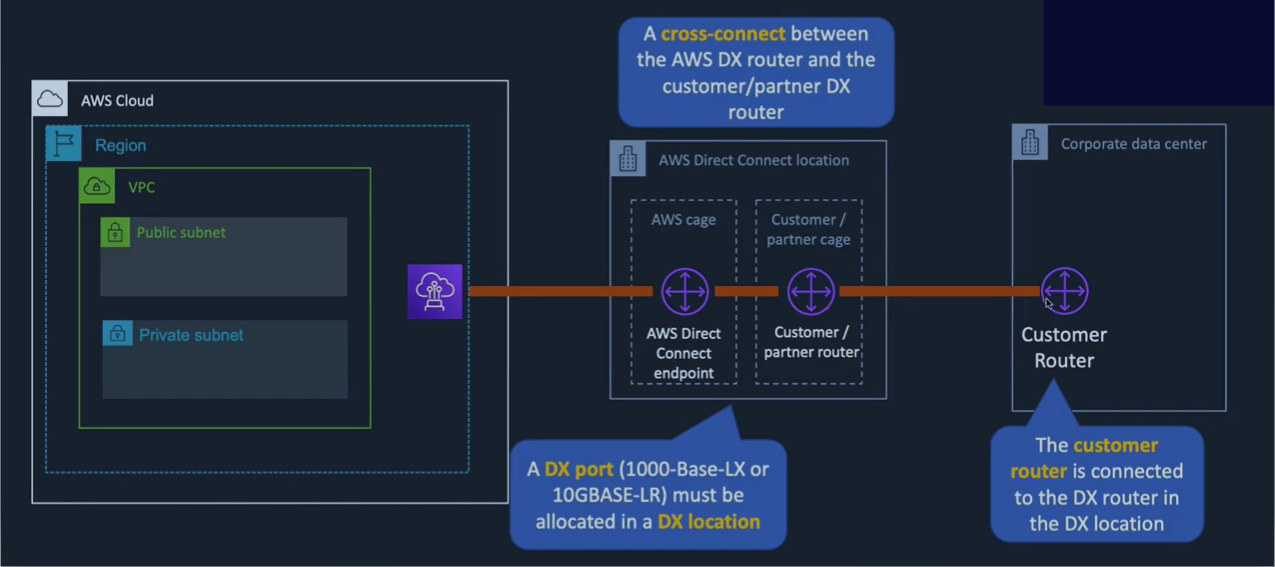
AWS will allocate private IP addresses (/30) in the 169.x.x.x range for the Border Gateway Protocol (BGP) session and will advertise the VPC Classless Inter-Domain Routing(CIDR) block over BGP. We can advertise the default route via BGP. A VPC VPN Connection creates encrypted network connectivity between your intranet and Amazon VPC over the Internet with the help of IPSec. This is very useful as DX connections are not inherently encrypted. VPN Connections can be configured quickly, have low to modest bandwidth requirements, and can tolerate the inherent variability in Internet-based connectivity.

*Sources: IEEE 802.1Q(* [*https://www.ieee802.org/802\_tutorials/2013-03/8021-IETF-tutorial-final.pdf*](https://www.ieee802.org/802_tutorials/2013-03/8021-IETF-tutorial-final.pdf) *) , AWS Direct Connect User guide(* [*https://docs.aws.amazon.com/directconnect/latest/UserGuide/dc-ug.pdf*](https://docs.aws.amazon.com/directconnect/latest/UserGuide/dc-ug.pdf) *), AWS Direct connect FAQs(* [*https://aws.amazon.com/directconnect/faqs/*](https://aws.amazon.com/directconnect/faqs/) *)*

3)

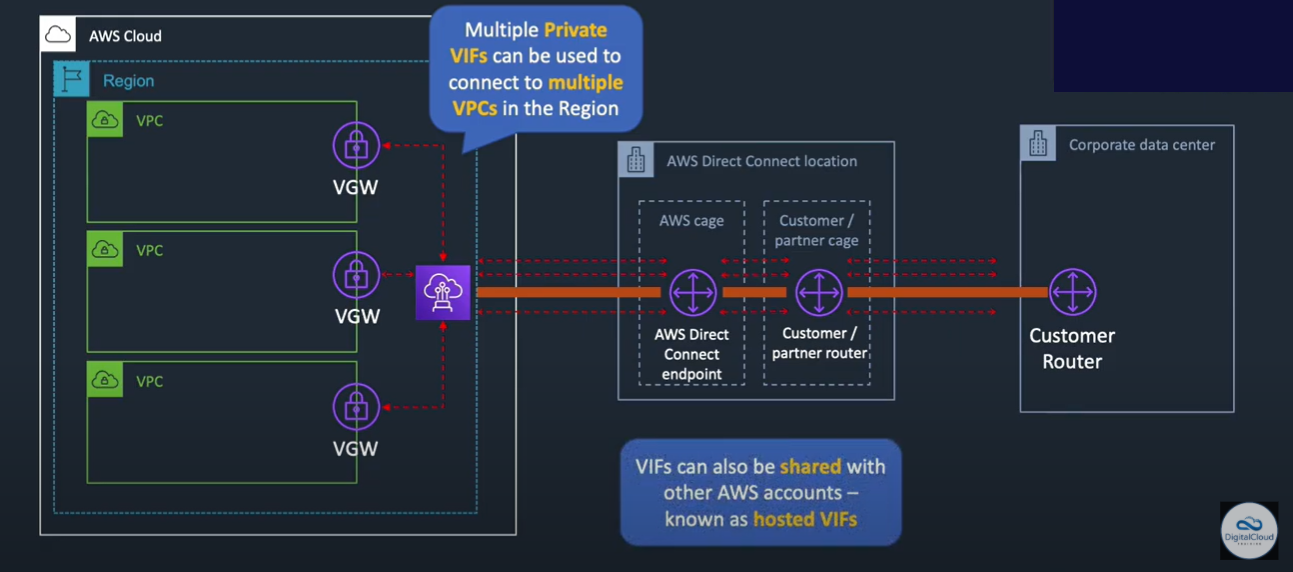
AWS direct connect is used to create a dedicated independent connection for an organization’s data center to AWS without relying on the Internet Service providers. This involves first connecting the organization’s data center routers to an AWS direct connect location , possibly with help from an Amazon partner Network (APN). Here, the customer cage which receives connection from the organization, which is in turn connected to the AWS cage. This connects to AWS system.

A virtual private cloud(VPC) exists in an AWS context within an AWS region – and can consist of several public or private subnets – each of which exist within availability zone(AZ). A VPC spans all AZs in the same region. The architecture described in the preceding two paragraphs in roughly illustrated below:



When you create a private virtual interface to a VPC, you will need a private virtual interface for each VPC, you want to connect. This connection requires the use of Border Gateway Protocol (BGP). To enable this connection you require (i) a public or private ASN, (ii) new unused VLAN, and (iii) a VPC Virtual Private Gateway (VGW) id (AWS will allocate private IPs (/30) in the 169.x.x.x range for the BGP session and will advertise the VPC CIDR block over BGP).

We can also connect several VPCs in a region using direct connect via VGW; as illustrated below:



We connect to the virtual private gateway in following steps:

i. Verify that the VLAN is not already in use on this connection.

ii. Open the AWS Direct Connect console at ( <https://console.aws.amazon.com/directconnect/> )

iii. In the Connections pane, select the connection to use, and then click Create Virtual Interface.

iv. In the Create a Virtual Interface pane, select Private.

v. Under Define Your New Private Virtual Interface, do the following:

a. In the Interface Name field, enter a name for the virtual interface.

b. In Interface Owner, select the My AWS Account option if the virtual interface is for your AWS account ID.

c. In the VGW list, select the virtual gateway to connect to.

d. In the VLAN # field, enter the ID number for your virtual local area network (VLAN); for example, a number between 1 and 4094.

e. To have AWS generate your router IP address and Amazon IP address, select Auto-generate peer IPs.

To specify these IP addresses yourself, clear the Auto-generate peer IPs check box, and then the Your router peer IP field, enter the destination IPv4 CIDR address that Amazon should send traffic to. In the Amazon router peer IP field, enter the IPv4 CIDR address you will use to send traffic to Amazon Web Services.

f. In the BGP ASN field, enter the Border Gateway Protocol (BGP) Autonomous System Number(ASN) of your gateway; for example, a number between 1 and 65534.

g. Select Auto-generate BPG key check box to have AWS generate one. To provide your own BGP key, clear the Auto-generate BPG key check box, and then in the BGP Authorization Key field, enter your BGP MD5 key.

vi. Click Continue, and then download your router configuration and configure your router.

*Sources: AWS Direct Connect - AWS Networking(*[*https://www.youtube.com/watch?v=jEcl5H8Ow\_8*](https://www.youtube.com/watch?v=jEcl5H8Ow_8)*), What is AWS direct connect(* [*http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html*](http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html) *), AWS Direct Connect User Guide(* [*http://awsdocs.s3.amazonaws.com/directconnect/latest/dc-ug.pdf*](http://awsdocs.s3.amazonaws.com/directconnect/latest/dc-ug.pdf) *)*

4)

a) Network address translation (NAT) is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

In AWS direct connect use cases, we often typically create 2 subnets within the VPC – one private and one public. The public subnet can be used to access Amazon S3 buckets, simple queue service(SQS), simple notification service(SNS),etc while the private one is used to access Amazon EC2 instances and resources that made available only the private VPC.

However, sometimes virtual private subnets also need internet access (to access a database server over the internet or to update some software). Herein, NAT gateway are used to connect the private subnets to internet. We create NATs in the public subnets. We also modify the route table for the private subnets to route all outbound internet traffic to the NAT. The NAT will replace the outgoing source IP address with the NAT device address and similarly, when the response traffic arrives from the internet NAT translates the addresses back to the corresponding private addresses for the subnet.

Nat will not be useful in cases where there are instances that require the use of static public IP addresses without Internet gateway to enable communication over the Internet as this scenario includes a virtual private cloud (VPC) with a single private subnet, and a virtual private gateway to enable communication with own network over an IPsec VPN tunnel.

*Sources: AWS - VPC Demo, Public & Private Subnets, Route Tables, Internet & NAT Gateways (* [*https://www.youtube.com/watch?v=tD9vDv0uyI8*](https://www.youtube.com/watch?v=tD9vDv0uyI8) *), Wikipedia(* [*https://en.wikipedia.org/wiki/Network\_address\_translation*](https://en.wikipedia.org/wiki/Network_address_translation) *), AWS VPC & Subnets | Amazon Web Services BASICS(* [*https://www.youtube.com/watch?v=bGDMeD6kOz0*](https://www.youtube.com/watch?v=bGDMeD6kOz0) *), How Network Address translation works(* [*https://computer.howstuffworks.com/nat.htm*](https://computer.howstuffworks.com/nat.htm) *)*

b)

The maximum possible connections a single NAT box can maintain = 216 = 65536

We know that, 4096 connections are reserved.

Hence, total no. of effective connection available in NAT box = 65536 – 4096 = **61440**

*Sources: textbook, What is the maximum number of connections a NAT box can support? (* [*https://philosophy-question.com/library/lecture/read/330664-what-is-the-maximum-number-of-connections-a-nat-box-can-support#0*](https://philosophy-question.com/library/lecture/read/330664-what-is-the-maximum-number-of-connections-a-nat-box-can-support#0) *)*

5)

a) To use AWS Direct Connect with Amazon VPC required the use of the Border Gateway Protocol (BGP) with an Autonomous System Number (ASN) and IP Prefixes. When you create a private virtual interface to a VPC, you will need a private virtual interface for each VPC, you want to connect. This connection requires the use of Border Gateway Protocol (BGP). Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet. BGP enables sending router decides on the shortest path to the destination based on the routing table lookup which was previously obtained from a “neighbor” and subsequently updated.

*Sources: Wikipedia(* [*https://en.wikipedia.org/wiki/Border\_Gateway\_Protocol*](https://en.wikipedia.org/wiki/Border_Gateway_Protocol) *), What is AWS direct connect(* [*http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html*](http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html) *), Network working group(* [*https://www.ietf.org/rfc/rfc1930.txt*](https://www.ietf.org/rfc/rfc1930.txt) *)*

b)

Yes, we can use our own ASN to connect to VPC.

An Autonomous System Number (ASN) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators. ASN are used to identify networks that present common, clearly defined routing policy to the Internet. In AWS direct connect we require an ASN to create a public or private virtual interface. We may pick any private ASN between 64512 to 65534 or we can use any public ASN owned by us.

*Sources: Wikipedia(* [*https://en.wikipedia.org/wiki/Autonomous\_system\_(Internet)*](https://en.wikipedia.org/wiki/Autonomous_system_(Internet)) *), AWS Direct Connect FAQs(*[*https://aws.amazon.com/directconnect/faqs/*](https://aws.amazon.com/directconnect/faqs/) *) and Network working group(* [*https://www.ietf.org/rfc/rfc1930.txt*](https://www.ietf.org/rfc/rfc1930.txt) *)*

c) A regional Internet registry (RIR) is an organization that manages the allocation and registration of Internet number resources within a region of the world. Internet number resources include IP addresses and autonomous system (AS) numbers. The regional Internet registry system evolved, eventually dividing the responsibility for management to a registry for each of five regions of the world. The regional Internet registries are informally liaised through the unincorporated Number Resource Organization (NRO), which is a coordinating body to act on matters of global importance.

To establish ASN for Sapporo, Japan it would be best to approach Asia Pacific Network Information Centre (APNIC). APNIC is the regional Internet address registry (RIR) for the Asia-Pacific region, and provides number resource allocation and registration services that support the global operation of the Internet.

*Sources: Wikipedia(* [*https://en.wikipedia.org/wiki/Regional\_Internet\_registry*](https://en.wikipedia.org/wiki/Regional_Internet_registry) *,* [*https://en.wikipedia.org/wiki/APNIC*](https://en.wikipedia.org/wiki/APNIC) *), APNIC(* [*https://www.apnic.net/*](https://www.apnic.net/) *)*

d)

The main problem with Border Gateway Protocol (BGP) is that it relies on trust between network operators that they will secure their systems correctly and not send problematic data; instead of including direct security mechanisms. This situation is vulnerable to both occasional mistakes as well as to malicious attackers trying to distort the routing tables used by BGP.

There are many means possible for supporting secure and private communication, transaction protection and identity assertion and management. These include Internet PKI used for secure web browsing as well as for other applications. DANE is a new protocol that uses DNSSEC to allow owners to assert their own digital certificates, and therefore potentially incorporate the functionality of the Internet PKI into the global DNS.PKI for emails and RPKI for Regional Internet registry(RIR) to validate holders of IP resources and DNSSEC to validate DNS queries – are example of safety mechanism we can resort to secure the BGP.

*Sources: Introduction to PKIs and CAs(* [*https://www.internetsociety.org/resources/deploy360/2017/introduction-to-pkis-cas/*](https://www.internetsociety.org/resources/deploy360/2017/introduction-to-pkis-cas/) *), The long life of a quick “fix” (* [*https://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/*](https://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/) *)*

6)

Given:

* Required connection rate between 2 data centers = 150 Mbps (bi-directional)
* Time this connection needs to be active = 2 hrs = 2\*60\*60 = 7200 sec
* Data carried in disc = 7GB
* Dist. between the centers = 5.5km = 5500 m
* Speed of dogs = 18 kmph = 5 m/sec

Therefore,

* Required volume of data transfer per day(uni-directional) = ( 150\*7200/8 ) MB = 135 GB
* Capacity of one dog in one errand = (3 \* 7GB) = 21 GB
* Time for 1 errand = 5500/5 = 1100 s
* Total no. of errand dog can do in 2hr = 7200/1100 = 6.54
* Capacity for data transfer for dog in 2 hrs = 6.54 \* 21= 137.45 GB

(Since, the dogs Alpha and Beta have same capabilities and speeds, and can synchronize to carry data in both direction, we can consider one pipe to be analogous to 1 dog)

From above calculation, its evident that the dogs can manage 137.45 GB data transfer(uni-directionally) while the required volume in 135 GB unidirectionally. Hence the dogs can cover the required volume.

Therefore, this solution will **work**, and the dogs can replace the pipes.