CS 524 Homework #3

This homework contains both technical and business-related problems, for the total of 100 points. Note that this homework requires a good deal of a self-study to understand the subject matter fully. To understand the material and complete the homework should take the two weeks allotted, so start working on it now! To this end, consider it a typical every-day problem you would need to solve if you worked as a product manager in a large company or ran a start-up company yourself. You also need to complete reading Chapter 4.

1. **(10 points) Given the token bucket size, b bytes; token rate, r bytes/sec; and maximum output rate M bytes/sec, what is the maximum burst time T?**

The token bucket algorithm is based on an analogy of a fixed capacity bucket into which tokens, normally representing a unit of bytes or a single packet of predetermined size, are added at a fixed rate. When a packet is to be checked for conformance to the defined limits, the bucket is inspected to see if it contains sufficient tokens at that time. The total number of appropriate tokens (length of packet in bytes), are removed and the packet is passed (for transmission).

Steps to calculate burst time are:
1. A token is added to the bucket every 1/r second
2. It is given that the bucket size is b bytes means the bucket can hold at the most b tokens and if a token arrives when the bucket is full will be discarded.
3. If a packet of 'n bytes' arrives, then 'n' tokens will be removed from the bucket and the packet is sent to the network. If fewer than 'n' tokens are available, then no tokens will be removed from the bucket.
4. M is a maximum output rate and r is a token rate then Tmax (maximum burst time) is:
Tmax = b/(M-r), provided r<M; otherwise Tmax = ∞

(**Reference**: https://en.wikipedia.org/wiki/Token_bucket)

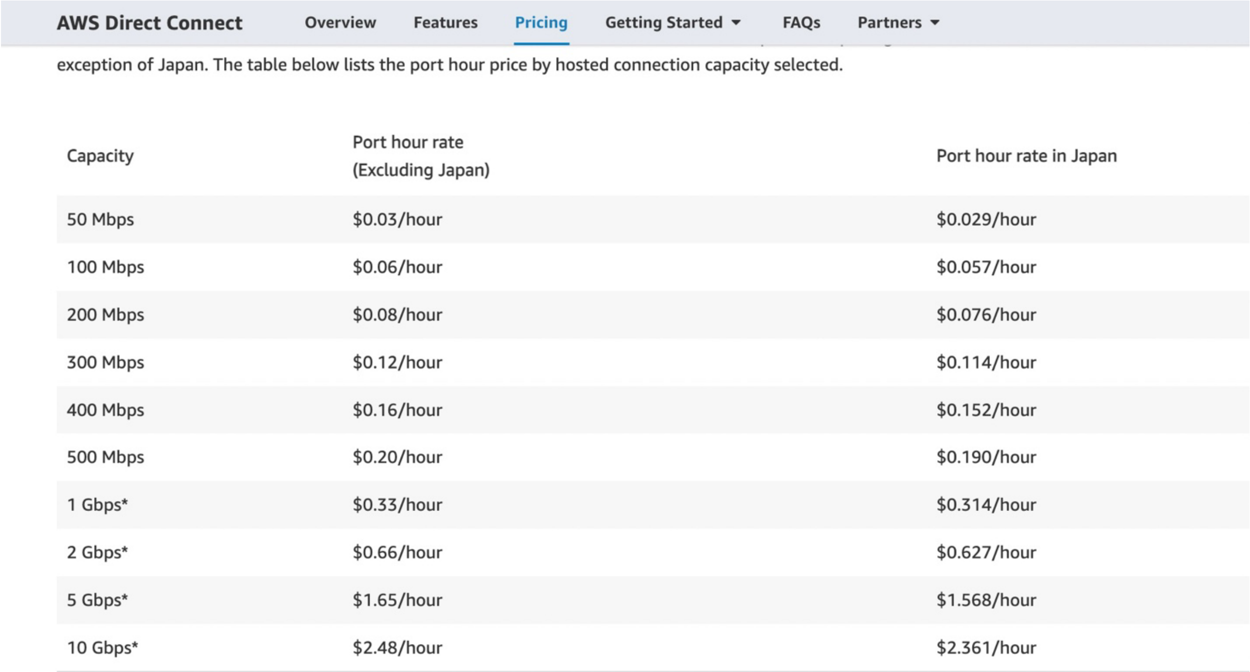
2. (50 points) Study the AWS Direct Connect service and answer the following questions:

a. (business) You own a company with a data center in Sapporo, Japan. Which company would you choose to connect this location to the Amazon service? Can you find out about pricing and QoS guarantees? (This may require some research. If you are unable to find the exact answers, describe what you have done to find them and what remains to be done.)

For Sapporo, Japan. I would choose to connect Equinix, Inc among other partners to connect this location to the Amazon Web Services. As with Equinix data centers Offers many options for high-performance, private access to AWS Direct Connect. Depending upon the data volume, AWS Direct connect customers can cut data transfer costs by two to ten times.
Following are the benefits of Equinix:
1. It provides a flexible range of speeds (50, 100, 200, 300, 400, and 500 Megabits per second) with Virtual Connections (VCs) via Equinix Cloud Exchange.

2. Provides cross connections either 1 or 10 Gigabits per second connections.
3. Offers latest technology capabilities and has the facility to migrate to hybrid cloud computing.

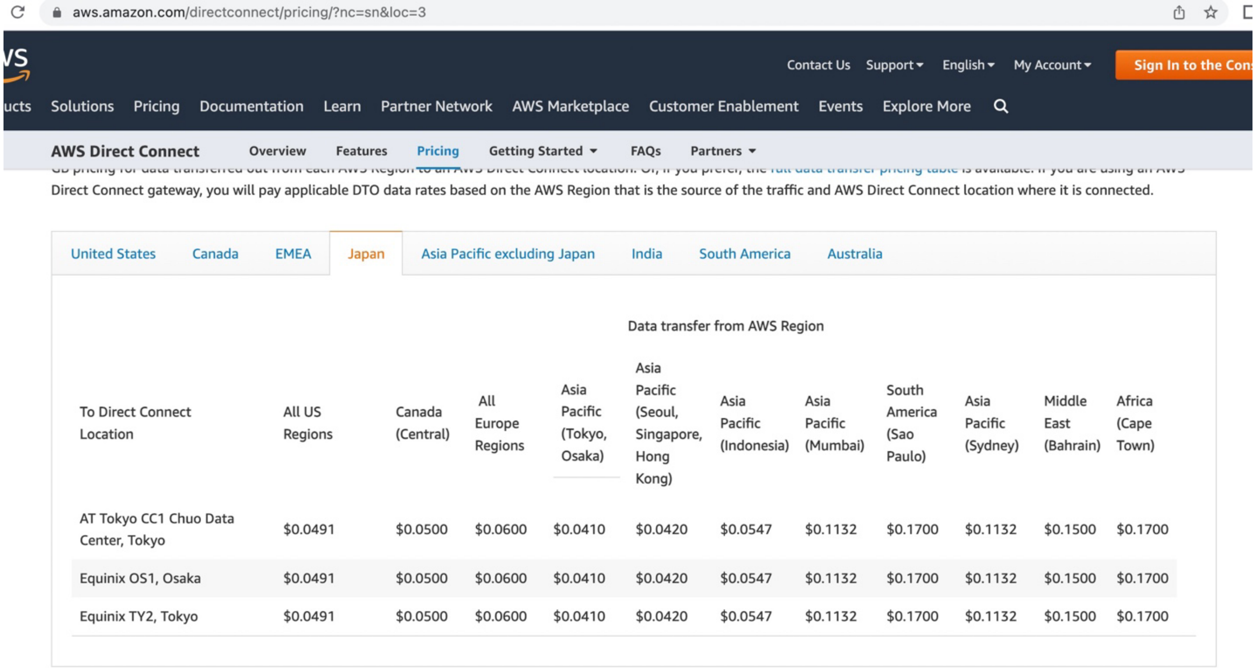
Hosted Connection port hour pricing is consistent across all AWS Direct Connect locations globally apart from Japan. The table below lists the port hour price by hosted connection capacity selected:



exception of Japan. The table below lists the port hour price by hosted connection capacity selected.

Capacity	Port hour rate (Excluding Japan)	Port hour rate in Japan
50 Mbps	$0.03/hour	$0.029/hour
100 Mbps	$0.06/hour	$0.057/hour
200 Mbps	$0.08/hour	$0.076/hour
300 Mbps	$0.12/hour	$0.114/hour
400 Mbps	$0.16/hour	$0.152/hour
500 Mbps	$0.20/hour	$0.190/hour
1 Gbps*	$0.33/hour	$0.314/hour
2 Gbps*	$0.66/hour	$0.627/hour
5 Gbps*	$1.65/hour	$1.568/hour
10 Gbps*	$2.48/hour	$2.361/hour

Data Transfer out Prices for Japan:



Direct Connect gateway, you will pay applicable DTO data rates based on the AWS Region that is the source of the traffic and AWS Direct Connect location where it is connected.

Data transfer from AWS Region

To Direct Connect Location	All US Regions	Canada (Central)	All Europe Regions	Asia Pacific (Tokyo, Osaka)	Asia Pacific (Seoul, Singapore, Hong Kong)	Asia Pacific (Indonesia)	Asia Pacific (Mumbai)	South America (Sao Paulo)	Asia Pacific (Sydney)	Middle East (Bahrain)	Africa (Cape Town)
AT Tokyo CC1 Chuo Data Center, Tokyo	$0.0491	$0.0500	$0.0600	$0.0410	$0.0420	$0.0547	$0.1132	$0.1700	$0.1132	$0.1500	$0.1700
Equinix OS1, Osaka	$0.0491	$0.0500	$0.0600	$0.0410	$0.0420	$0.0547	$0.1132	$0.1700	$0.1132	$0.1500	$0.1700
Equinix TY2, Tokyo	$0.0491	$0.0500	$0.0600	$0.0410	$0.0420	$0.0547	$0.1132	$0.1700	$0.1132	$0.1500	$0.1700

QoS Guarantees:
AWS Direct Connect does not provide managed QoS functionality. The idea that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. QoS is of particular concern for the continuous transmission of high-bandwidth video and multimedia information. Dependably transmitting this kind of content is difficult in public networks using standard best-effort protocols.

Reliability – All Equinix IBX data centers are equipped with full UPS power, back-up systems and N+1 (or greater) redundancy, with a proven, industry-leading >99.99999% uptime record.

Power Density – With robust heating, ventilation and air conditioning (HVAC) systems, Equinix IBX data centers exceed the requirements of even the most power-hungry deployments.

Security – Every Equinix IBX data center utilizes an array of security equipment, techniques and procedures to control, monitor, and record access to the facility, including individual cages.

Recovery – IBXflex Space provides operations centers and storage space when we need it; Equinix Smart Hand offers 24-hour access to qualified technical support—with Equinix, we can maintain our mission-critical operations and equipment under any circumstances. It provides:
~High average uptime—There IBX data centers boast an industry-leading track record of >99.99999%.
~Proven expertise—They help to configure and support high-power density deployments.

The largest worldwide footprint provides 14M+ ft2 of data center space across 40 markets in 21 countries on 5 continents.

More than 1,400+ networks covered for interconnection and traffic exchange via direct cross connects, peering and cloud services.

(**Reference**: https://aws.amazon.com/directconnect/partners/#apac, https://www.equinix.com/partners/aws, http://www.equinix.com/services/data-centers-colocation/, https://aws.amazon.com/directconnect/pricing/, https://docs.equinix.com/en-us/Content/glossary.htm)

b. (technical) As you have noticed, the AWS Direct Connect service description refers to the IEEE standard 802.1q. Use the Internet resources to find out about this standard (which you should be able to find at the Stevens Library) and explain how a dedicated connection can be partitioned into multiple virtual interfaces so as to allow you to "use the same connection to access public resources such as objects stored in Amazon S3 using public IP address space, and private resources such as Amazon EC2 instances running within an Amazon Virtual Private Cloud (VPC) using private IP space." Quote the resources (web pages or papers) that you have used.

One can establish 1 Gbps or 10 Gbps dedicated network connections between AWS and any of the AWS Direct Connect locations with AWS Direct Connect. A dedicated connection can be partitioned into multiple logical connections by using industry-standard 802.1QVLANs. We can use the same connection to access public resources, such as objects stored in Amazon Simple Storage Service (Amazon S3) that use public IP address space, and private resources, such as Amazon EC2 instances that are running within a VPC using private IP space—all while maintaining network separation between the public and private environments. We can choose a partner from the AWS Partner Network (APN) to integrate the AWS Direct Connect endpoint in an AWS Direct Connect location with our remote networks.

We may combine all these different options in any combination for the business and security policies. For example, we could attach a VPC to our existing data center with a virtual private gateway and set up an additional public subnet to connect to other AWS services that dont run within the VPC, such as Amazon S3, Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS).

AWS allocates private IPs (/30) in the 169.x.x.x range for the BGP session and will advertise the VPC CIDR block over BGP. One can use the default route via BGP. A VPC VPN Connection creates encrypted network connectivity between our intranet and Amazon VPC over the Internet with the help of IPSec.

VPN Connections can be configured quickly which is a benefit, have low to modest bandwidth requirements, and can tolerate the inherent variability in Internet-based connectivity. AWS Direct Connect does not involve the Internet; instead, it uses dedicated, private network connections between our intranet and Amazon VPC.

(**Reference**: http://docs.aws.amazon.com/directconnect/latest/UserGuide/dc-ug.pdf, https://aws.amazon.com/directconnect/faqs/)

3. (10 points) Describe how the AWS Direct Connect service can be used with the Amazon Virtual Private Cloud (VPC).

When using AWS Direct Connect, we can connect to VPCs deployed in any AWS Region and Availability Zone. AWS Direct Connect links our internal network to an AWS Direct Connect location over a standard 1 gigabit or 10 gigabit Ethernet fiber-optic cable. Router is connected on one end of the cable, the other to an AWS Direct Connect router.

Virtual interfaces can be created directly to the AWS cloud (for example, to Amazon EC2 and Amazon S3) and to Amazon VPC, bypassing Internet service providers in our network path. An AWS Direct Connect location provides access to AWS in the Region with which it is associated. We can use a single connection in a public Region or AWS GovCloud (US) to access public AWS services in all other public Regions.
When we create a private virtual interface to a VPC, we will need a private virtual interface for each VPC, we want to connect. This connection requires the use of Border Gateway Protocol

(BGP).
The following information is needed to complete the connection:
-A public or private ASN. For public ASN we must own it else if we are using a private ASN, it must be in the 65000 range.
-A new unused VLAN tag that we select
-The 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 advertise the default route via BGP).

The Virtual Private Gateway to connect:
-Verify the VLAN is not in use on the same connection.
-Open the AWS Direct Connect console.
-In the connection pane, choose the connection to use, and then click Create Virtual Interface.
-In the Create a Virtual Interface pane, choose Private.
-Under Define Your New Private Virtual Interface, Enter a name for the virtual interface in the Interface Name field.
•In the Interface Owner, select the My AWS Account option if the virtual interface is for your AWS account ID.
• For the VGW list, choose the virtual gateway to connect to.
•In the VLAN # field, enter the ID number for your virtual local area network (VLAN); for example, a number between 1 and 4094.
•To have AWS generate your router IP address and Amazon IP address, select Auto-generate peer IPs.
In the BGP ASN filed, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway; for example, a number between 1 and 65534.
•Select Auto-generate BGP key check box to have AWS generate one.

-To provide your own BGP key, clear the Auto-generate BGP key check box, and then in the BGP Authorization Key field, enter your BGP MD5 key.
-Then download the router configuration and configure the router.

An AWS Direct Connect location provides access to Amazon Web Services in the region it is associated with, as well as access to other US regions. For example, one can provision a single connection to any AWS Direct Connect location in the US and use it to access public AWS services in all US Regions and AWS GovCloud (US). The following diagram shows how AWS Direct Connect interfaces with your network.

(**Reference**: http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html, https://aws.amazon.com/directconnect/faqs/)

4. (10 points) Note that Amazon VPC provides NAT.
a. Explain why you would want to use NAT for a virtual private subnet with the Amazon Direct Connect service. Do you see any cases where you would not want to use it?

Network Address Translation (NAT) is a process of re-mapping one of the IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device. For example, router, which act as an agent between a local (or private network) and the internet (or public network), which represent a unique IP address to public network for entire group of computers on private network.

We use NAT for virtual private subnet with the Amazon Direct Connect Services to enable instances in a private subnet to connect to the Internet (for example, software updates) or other AWS services, but abstain the Internet from initiating connections with instances. A NAT forwards traffic from the instances in the private subnet to the Internet or other AWS services, and then sends the response back to the instances. When traffic leads towards the Internet, the source IP address is replaced with the NAT device's address and likewise, when response traffic moves towards those instances, the NAT devices translates the address back to those instances' private IP addresses.

The cases where we the uses of NAT are bad, when a user is working with instances that require the use of static public IP address and when there is no Internet gateway to enable communication over the Internet, 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.

(**Reference**: https://en.wikipedia.org/wiki/Network_address_translation,
http://computer.howstuffworks.com/nat.htm,
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpcnat.html)

b. What is the maximum number of connections a single NAT box can maintain? (You need to check the specifications of the three existing transport-layer protocols on the Internet: TCP, UDP, and SCTP, and also keep in mind that the first 4,096 ports have been reserved.)

The maximum number of connections that a single NAT box can maintain is 216 ie 65,536. The first 4,096 ports are reserved, so the effective number of maximum connections that can be used are 65,536-4096 ie 61440.

(**Reference**: Cloud Computing: Business Trends and Technologies)

5. (10 points) Read RFC 1930 (http://www.ietf.org/rfc/rfc1930.txt) and also a Washington Post article, https://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/. and answer the following questions:

a. To use AWS Direct Connect with Amazon VPC, the Border Gateway Protocol is required. Why?

A standardized exterior gateway, Border Gateway Protocol is a protocol designed to exchange routing and reachability information among autonomous systems (AS) on the internet. Uses of BGP include communication between two routing domains (to exchange routes from VPC to private network). BGP enables sending router decides on the shortest path to the destination based on the routing table lookup that was previously obtained from a “neighbor” and subsequently updated.

(**References**: https://en.wikipedia.org/wiki/Border_Gateway_Protocol, https://aws.amazon.com/directconnect/faqs/)

b. Can you use your 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. AWS Direct Connect requires an ASN to create a public or private virtual interface. We may use a public ASN which we own, or we can pick any private ASN between 64512 to 65534.

Yes, it is possible for us to use our own ASN to connect to VPC.

(**References**: https://en.wikipedia.org/wiki/Autonomous_system_(Internet), https://aws.amazon.com/directconnect/faqs/)

c. Which RIR would you go to when you need to establish an ASN for your data center in Sapporo, Japan?

Regional Internet Registry (RIR) is an organization which manages the allocation and registration of Internet number resources within a particular region of the world. Internet number resources include IP addresses and autonomous system (AS) numbers.

To establish an ASN for the data center in Sapporo, Japan, I shall use the Asia Pacific Network Information Centre (APNIC). APNIC is a membership-based organization whose members include Internet Service Providers, National Internet Registries, and similar organizations. It provides number resource allocation and registration services that support the global operation of the Internet. Membership-based
The main functions of APNIC are:

1. Allocating IPv4 and IPv6 address space, and Autonomous System Numbers,
2. maintaining the public Whose Database for the Asia Pacific region,
3. reverse DNS delegations,
4. representing the interests of the Asia Pacific Internet community on the global stage.

(**References**: https://en.wikipedia.org/wiki/Regional_Internet_registry, https://en.wikipedia.org/wiki/Asia-Pacific_Network_Information_Centre, https://www.apnic.net/)

d. What security problems you will have to deal with using BGP, and what how are you going to address them?

The security problem with BGP is that the protocol doesn't directly include security mechanisms, also it is based largely on trust between network operators to secure their systems correctly and not send incorrect data. Issues happen, problems can arise if malicious attackers were to try to affect the routing tables used by BGP. There are multiple commonly used mechanisms for supporting secure and private communication, transaction protection, identity assertion and management. Some of them are the Internet PKI used for secure web browsing, also used for other applications, PKI for e-mail, RPKI used by Regional Internet Registries to assert the holders of IP resources, and DNSSEC which can be used to validate DNS queries. 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.

(**References:** https://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/, https://aws.amazon.com/blogs/networking-and-content-delivery/how-aws-is-helping-to-secure-internet-routing/)

6. (10 points) St. Bernard dogs (a breed originated in a Swiss monastery to save the travelers stranded in snow) have been trained to run on their missions in snow-covered mountains with flasks of brandy attached to their necks. (See the picture below.)

Now, you retrain your company's two St. Bernards, named Alpha and Beta, to carry data in DVD ROM disks. (The disks, in bundles of three, are attached to a dog's necks where the flask used to be, so one dog can carry three disks.)

Each disk stores 7 Gb of data. Both Alpha and Beta run at a constant speed of 18 km/h. (1 Gb = 1,000 megabytes = 1,000,000 bytes.)

Your company has two data centers, which need to be interconnected with two 150-Mbps data pipes—one in each direction. The distance between the data centers is 5.5 km. (Mbps = megabits per second.)

Your task is to ensure that the data centers be interconnected. You can achieve that by

1) Building a physical network (very expensive, given the terrain);
2) Renting pipes from service providers (pretty expensive); or
3) Writing the data on DVDs, and then running Alpha and Beta between the data centers (in opposite directions), with CDs attached. This is free, and the dogs need to exercise anyway.

Can the dogs provide this service? (Assume that the pipes need to operate for only a couple of hours a day, so the dogs don't get tired. Ignore the overhead of writing and reading DVDs—it is smaller than the data communications overhead anyway.)

Bernard's Dogs carry three 7GB Data Disc, hence total data carried by dog is 7*3 = 21 GB
Dogs travel at Speed of 18 km/hr

Distance between data center is 5.5 km => Time taken by Dogs to travel to the data center
Time = Distance/Speed
= 5.5/18 h = (5.5*60*60/18) seconds
= 1100 sec

Time taken to transfer the data
Date Rate = Data/Time
= 21000/1100
= 19.09 Mbps

So yes, I believe Bernard's Dogs can provide the service same as renting pipes for free and one should opt for them.