Homework 3: CS 524

1. **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?**

ANS.

The token bucket model is designed to allow bursts. Here the flow out of the bucket is controlled by a valve. The state of the valve is determined by the condition of the token bucket.

a. The Token bucket receives quantities called tokens at a rate of r bytes/sec, and a token is added to the bucket every 1/r seconds.
b. The bucket can hold b bytes. (The tokens stop arriving when the bucket is full.)

Now, when exiting the token bucket, a token opens the output valve of the main bucket to allow the output of one byte, at which point the valve is closed. Consequently, no traffic is admitted when the token bucket is empty. Yet, if there is no traffic to output, the bottom hole of the token bucket is closed, and so the tokens are saved in the bucket until they start to overflow.

c. When a packet (network layer PDU) of n bytes arrives,
   - if at least n tokens are in the bucket, n tokens are removed from the bucket, and the packet is sent to the network.
   - if fewer than n tokens are available, no tokens are removed from the bucket, and the packet is non-conformant.

d. Let M be the maximum possible transmission rate in bytes/second.

Thus, maximum burst time T_{max} = b/(M-r)

(References: Textbook: Cloud Computing: Business Trends and Technologies, Token bucket - Wikipedia)

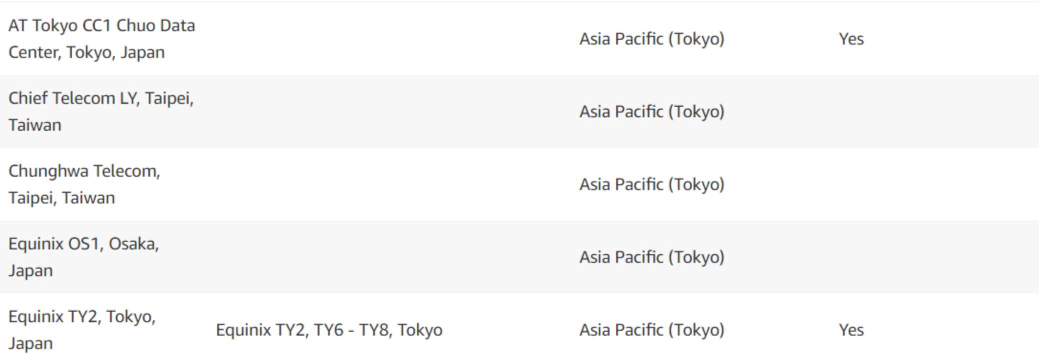
2.

a. **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.)**

ANS.

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations.



AT Tokyo CC1 Chuo Data Center, Tokyo, Japan		Asia Pacific (Tokyo)	Yes
Chief Telecom LY, Taipei, Taiwan		Asia Pacific (Tokyo)	
Chunghwa Telecom, Taipei, Taiwan		Asia Pacific (Tokyo)	
Equinix OS1, Osaka, Japan		Asia Pacific (Tokyo)	
Equinix TY2, Tokyo, Japan	Equinix TY2, TY6 - TY8, Tokyo	Asia Pacific (Tokyo)	Yes

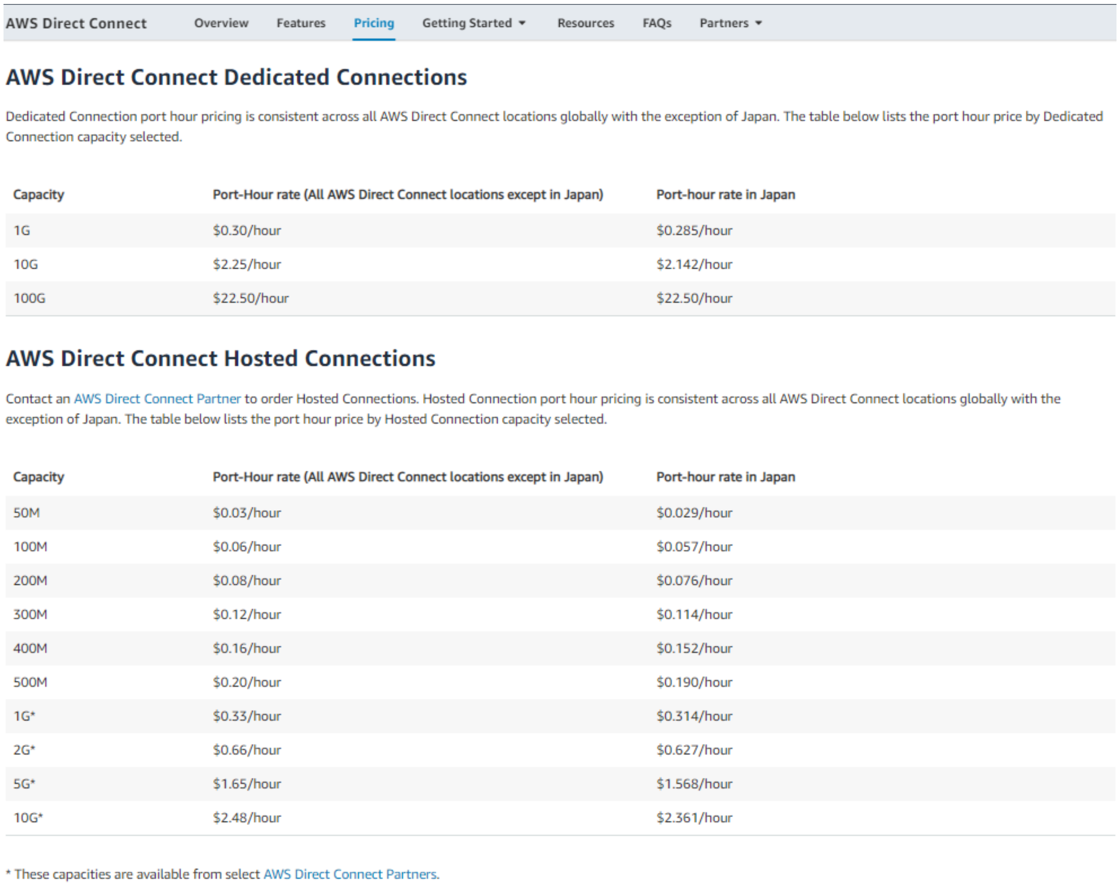
If I own a company with a data center in Sapporo, Japan; I would choose either the AT Tokyo CC1 Chuo Data Center or Equinix TY2 since both of them are dedicated 100G supported.

Direct Connect enables migration of workloads requiring higher connection speeds with lower latency for:

- Databases (e.g. Oracle, Microsoft SQL, etc.) by leveraging AWS tools
- Migration of on-premises VMware and SAP applications (e.g. HANA) to AWS
- Hybrid and multicloud architecture for mission-critical applications, especially those based on VMware and SAP
- Business continuity and disaster recovery environments
- High-performance, private access to AWS Direct Connect options are offered.
- Based on the data volume, AWS Direct Connect customers can cut data transfer costs by two to ten times.
- Offers Amazon Direct Connect Services covers more geographical locations than any other data center provider.

This will also allow guaranteed service with QoS like:

- These data centers, promise safety and security for your business, maintaining high-level service and zero-downtime operation.
- Using some of the most robust buildings with the strongest foundations in the industry worldwide.
- Multiple power feeds Direct cable connection to an ultra-high-voltage substation and power stations, backed up by UPS (Uninterruptible Power Supply), and Emergency Generators (EG)
- 24-hour, 365-day operations and monitoring system by highly experienced engineers and protected by multiple security levels.



AWS Direct Connect Dedicated Connections

Dedicated Connection port hour pricing is consistent across all AWS Direct Connect locations globally with the exception of Japan. The table below lists the port hour price by Dedicated Connection capacity selected.

Capacity	Port-Hour rate (All AWS Direct Connect locations except in Japan)	Port-hour rate in Japan
1G	$0.30/hour	$0.285/hour
10G	$2.25/hour	$2.142/hour
100G	$22.50/hour	$22.50/hour

AWS Direct Connect Hosted Connections

Contact an AWS Direct Connect Partner to order Hosted Connections. Hosted Connection port hour pricing is consistent across all AWS Direct Connect locations globally with the exception of Japan. The table below lists the port hour price by Hosted Connection capacity selected.

Capacity	Port-Hour rate (All AWS Direct Connect locations except in Japan)	Port-hour rate in Japan
50M	$0.03/hour	$0.029/hour
100M	$0.06/hour	$0.057/hour
200M	$0.08/hour	$0.076/hour
300M	$0.12/hour	$0.114/hour
400M	$0.16/hour	$0.152/hour
500M	$0.20/hour	$0.190/hour
1G*	$0.33/hour	$0.314/hour
2G*	$0.66/hour	$0.627/hour
5G*	$1.65/hour	$1.568/hour
10G*	$2.48/hour	$2.361/hour

* These capacities are available from select AWS Direct Connect Partners.

(References: AWS Direct Connect features (amazon.com),DATA CENTER INFORMATION | AT TOKYO Data Center, Amazon Web Services | Equinix Alliance Partners)

b. 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.

ANS.

Yes, AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations. Using industry standard 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces. This allows 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, while maintaining network separation between the public and private environments. Virtual interfaces can be reconfigured at any time to meet your changing needs.

A VPC VPN Connection utilizes IPSec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet. VPN Connections can be configured in minutes and are a good solution if you have an immediate need, 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 your intranet and Amazon VPC.

One may combine all these different options in any combination that make the most sense for one's business and security policies. For example, you could attach a VPC to your existing data centre with a virtual private gateway and set up an additional public subnet to connect to other AWS services that do not run within the VPC, such as Amazon S3, Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS). 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. A VPC VPN Connection creates encrypted network connectivity between your intranet and Amazon VPC over the Internet with the help of IPSec.

VPN Connections can be configured quickly, 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 dedicate, private network connections between your intranet and Amazon VPC.

(References: AWS Direct Connect features (amazon.com), https://aws.amazon.com/directconnect/faqs/, AWS Direct Connect Frequently Asked Questions (amazon.com))

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

ANS.

AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. With this connection, you can create virtual interfaces directly to public AWS services (for example, to Amazon S3) or to Amazon VPC, bypassing internet service providers in your network path. An AWS Direct Connect location provides access to AWS in the Region with which it is associated. You can use a single connection in a public Region or AWS GovCloud (US) to access public AWS services in all other public Regions.

The service can be used using:

1. Open the AWS Direct Connect console at https://console.aws.amazon.com/directconnect/v2/home.
2. In the navigation pane, choose **Virtual Interfaces**.
3. Choose **Create virtual interface**.
4. Under **Virtual interface type**, for **Type**, choose **Private**.
5. Under **Private virtual interface settings**, do the following:
    1. For **Virtual interface name**, enter a name for the virtual interface.
    2. For **Connection**, choose the Direct Connect connection that you want to use for this interface.
    3. For **Gateway type**, choose **Virtual private gateway**, or **Direct Connect gateway**.
    4. For **Virtual interface owner**, choose **Another AWS account**, and then enter the AWS account.
    5. For **Virtual private gateway**, choose the virtual private gateway to use for this interface.
    6. For **VLAN**, enter the ID number for your virtual local area network (VLAN).
    7. For **BGP ASN**, enter the The Border Gateway Protocol Autonomous System Number of your on-premises peer router for the new virtual interface.

       The valid values are 1-2147483647.
6. Under **Additional Settings**, do the following:
    1. To configure an IPv4 BGP or an IPv6 peer, do the following:

       [IPv4] To configure an IPv4 BGP peer, choose **IPv4** and do one of the following:

        - To specify these IP addresses yourself, for **Your router peer ip**, enter the destination IPv4 CIDR address to which Amazon should send traffic.
        - For **Amazon router peer ip**, enter the IPv4 CIDR address to use to send traffic to AWS.

       [IPv6] To configure an IPv6 BGP peer, choose **IPv6**. The peer IPv6 addresses are automatically assigned from Amazon's pool of IPv6 addresses. You cannot specify custom IPv6 addresses.
    2. To change the maximum transmission unit (MTU) from 1500 (default) to 9001 (jumbo frames), select **Jumbo MTU (MTU size 9001)**.
    3. (Optional) Add or remove a tag.

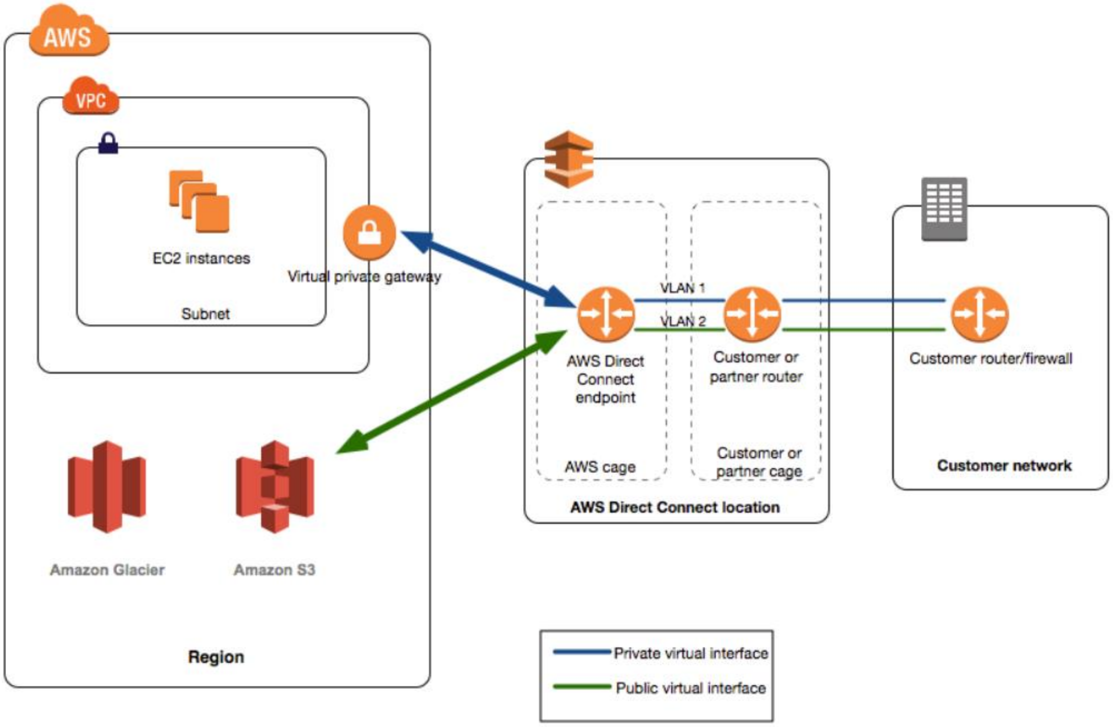
[Add a tag] Choose **Add tag** and do the following:

- For **Key**, enter the key name.
- For **Value**, enter the key value.

[Remove a tag] Next to the tag, choose **Remove tag**.

7. Choose **Create virtual interface**.
8. Download the router configuration for your device. For more information, see Downloading the router configuration file

The following diagram shows how AWS Direct Connect interfaces with your network.



(References: What is AWS Direct Connect? - AWS Direct Connect (amazon.com), Creating a virtual interface - AWS Direct Connect (amazon.com), https://aws.amazon.com/directconnect/faqs/)

4. Note that Amazon VPC provides NAT.

NAT, or network address translation, is a function embedded in even the simplest of SOHO routers. Simply put, NAT hides your device's "real" address from the network by translating this address to a different address for network communications, thereby supplying a measure of security.

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?

ANS.

We use NAT to enable instances in a private subnet to connect to the internet (for example, for software updates) or other AWS services, but prevent the internet from initiating connections with the instances. A NAT device 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 goes to the internet, the source IPv4 address is replaced with the NAT device's address and similarly, when the response traffic goes to those instances, the NAT device translates the address back to those instances' private IPv4 addresses.

You can use either a managed NAT device offered by AWS, called a NAT gateway, or you can create your own NAT device in an EC2 instance, called a NAT instance. We recommend NAT gateways, because they provide better availability and bandwidth over NAT instances. The NAT gateway service is also a managed service that does not require your administration efforts.

There cases where NAT shouldn't be used. Doing any Web-based functions that require passing the IP address in the body of the message can have problems working through NAT.

(References: NAT devices for your VPC - Amazon Virtual Private Cloud, NAT: the good, the bad and the ugly | Network World)

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.)

ANS.

The maximum number of connections that a single NAT box can maintain is 2^{16}. Since the port number—the key to an entry—is 16 bits long, and the first 4096 ports are reserved, the upper bound for the number of entries is equal to $2^{16} - 4096 = 61, 440$.

(References: Textbook: Cloud Computing: Business Trends and Technologies)

5. **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?

ANS.

We require Border Gateway Protocol with an Autonomous System Number and IP prefixes for connecting AWS Direct Connect with Amazon VPC.

Border Gateway Protocol (BGP) is the postal service of the Internet. When someone drops a letter into a mailbox, the postal service processes that piece of mail and chooses a fast, efficient route to deliver that letter to its recipient. Similarly, when someone submits data across the Internet, BGP is responsible for looking at all of the available paths that data could travel and picking the best route, which usually means hopping between autonomous systems.

BGP is the protocol that makes the Internet work. It does this by enabling data routing on the Internet.

(References: What Is BGP? | BGP Routing Explained | Cloudflare, AWS Direct Connect Frequently Asked Questions (amazon.com))

b. Can you use your own ASN to connect to VPC?

ANS.

Yes, you can use your own ASN to connect to VPC. Autonomous System numbers are used to identify networks that present a clearly defined external routing policy to the Internet. AWS Direct Connect requires an ASN to create a public or private virtual interface. You may use a public ASN which you own, or you can pick any private ASN number between 64512 to 65535 range.

(References: AWS Direct Connect Frequently Asked Questions (amazon.com))

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

ANS.

An RIR is an organization that manages and controls Internet addresses in a specific region, usually a country and sometimes an entire continent. RIRs control assigning and distributing IP addresses and domain registrations. As the Internet expanded throughout the world, greater organization was needed to handle the demand for IP addresses for the growing millions of online users.

We would go to APNIC RIR to establish an ASN for our data center in Sapporo, Japan

The Asia-Pacific Network Information Centre—APNIC: Responsible for the administration of Internet addresses and domains for Asia and the Pacific Rim. Founded in Tokyo, Japan, APNIC was the second RIR to be established. APNIC relocated to Brisbane, Australia, in 1998.

(References: What is an RIR? (whatismyipaddress.com))

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

ANS.

The creation of BGP, which relies on individual networks continuously sharing information about available data links, helped the Internet continue its growth into a worldwide network. But BGP also allows huge swaths of data to be “hijacked” by almost anyone with the necessary skills and access.

The main reason is that BGP, like many key systems on the Internet, is built to automatically trust users — something that may work on smaller networks but leaves a global one ripe for attack.

The major problems are:

- BGP route manipulation
- BGP route hijacking
- BGP denial-of-service (DoS)

To effectively secure BGP routing, there are proposals like:

- Resource Public Key Infrastructure (RPKI). This allows providers that hold large blocks of internet addresses to stipulate which networks can announce a direct address block connection, reducing the chance of cybercriminal networks calling the shots.
- BGP Origin Validation. Using RPKI information, routers can filter out route announcements that aren’t from authorized locations.
- BGP Path Validation. Also called BGPsec, the idea here is to use digital router signatures to ensure that traffic only crosses authorized networks. This kind of

path monitoring should help eliminate the ability of attackers to carry out undetected hijacks.

(References: Quick fix for an early Internet problem lives on a quarter-century later | The Washington Post, Agencies, Assemble! NIST and DHS Join Forces for BGP Security (securityintelligence.com))

6. St. Bernard's 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. 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.)

ANS.

Given,

No of St. Bernard's Dogs = 2

Each carry three 7GB Data Disc = 7*3

= 21 GB each,

For two dogs = 21 * 2

= 48 GB

Dog's Speed = 18 km/hr.

Distance between data center = 5.5 km

= 5500 m

Time = Distance/Speed

Time Taken to reach Data center = 5.5/18 km/hr.

= 1100 s

Data Rate for transfer of data = Data transferred/Time taken

= 48*1000*8/1100

= 168000/1100

= 305.455 Mbps

Thus St. Bernard's Dogs can theoretically transfer data twice as fast as the pipe and assuming it is more expensive then writing to the disk and transferring data.