CS 524 Homework #3

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?

Solution: A token bucket is a formal definition of a rate of transfer. It has three components: a burst size b, a mean rate r, and a time interval (T). Although the mean rate is generally represented as bits per second, any two values may be derived from the third by the relation shown as follows:

mean rate(r) = burst size(b) / time interval (T)

Here are some definitions of these terms:

- Mean rate—Also called the committed information rate (CIR), it specifies how much data can be sent or forwarded per unit time on average.
- Burst size—Also called the Committed Burst (Bc) size, it specifies in bits (or bytes) per burst, how much traffic can be sent within a given unit of time to not create scheduling concerns.
- Time interval—Also called the measurement interval, it specifies the time quantum in seconds per burst.

The maximum burst *M* can last for b/(M-r) seconds

Example: if b=20 bytes; M=5 bytes/sec and r=1 bytes/sec;

T=b/(M-r) = 20/(5-1)=20/4=5 seconds

Source:
[https://www.cisco.com/c/en/us/td/docs/ios/qos/configuration/guide/12_2sr/qos_12_2sr_book/policing_shping_oview.html]

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.)
   b. (technical) As you have noticed, the AWS Direct Connect service description refers to the IEEE standard 802.1q. Read this standard (which you should be able to find at http://www.ismlab.usf.edu/dcom/Ch3_802.1Q-2005.pdf or 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."

Solution:

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.

It has the following benefits:

- Reduces your bandwidth cost
- Consistent Network performance
- Compatible with all AWS Services
- Private Connectivity to your Amazon VPC
- Elastic

a. There are three locations in Japan which provide connectivity, two are located in Tokyo and one in Osaka. As geographically, Tokyo is much closer to Sapporo than Osaka, I would choose Equinix located in Tokyo.
    - Equinix's interconnection platform provides global access to AWS Direct Connect in 27 business-rich markets. AWS Direct Connect avoids the public Internet and guarantees private connectivity and complete integration between cloud services and commercial applications.
    - AWS Direct Connect plus Equinix interconnection is an ideal combination that allows hybrid cloud architectures to improve network performance, reduce operating costs and increase security.

Pricing can be shown as:

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.

- AWS Direct Connect, which operates on the Equinix Platform, offers unmatched benefits for cloud infrastructures: directing business applications and data in different locations with performance, security and scale.

- Improve value for AWS customers:

✓ Latency-sensitive applications and workloads require predictable performance and consistent, high-quality user experience.

✓ The implementation of Interconnection Oriented Architecture ™ (IOA ™) on the Equinix Platform, to take advantage of AWS Direct Connect, offers you the following benefits:

  - Predictable performance and user experience with dedicated direct connections, low latency and bandwidth for AWS

  - Improved compliance by connecting to AWS privately and maintaining data in the region, without going through the public Internet

  - Enabling a hybrid cloud that allows companies to keep private clouds and manage confidential data in secure Equinix data centers near AWS, while taking advantage of their flexibility, scalability and cost savings

QoS guarantees:

- AWS Direct Connect services are currently offered at Equinix International Business Exchange ™ (IBX®) data centers located in Amsterdam, Chicago, Dallas, Frankfurt, London (EU West - Ireland and EU West - London), Los Angeles, Munich , Osaka, Sao Paulo, Seattle, Silicon Valley, Singapore, Sydney, Tokyo, Hong Kong, Washington DC / Northern Virginia, Dubai, Helsinki, Madrid, Manchester, Paris, Warsaw, Stockholm, Miami, Rio de Janeiro, GovCloud: covering more markets than any other data center provider.

- Direct Connect for AWS GovCloud is available as an exclusive connection on the SV5 of Equinix, San José. Equinix customers in ECXF globally enabled locations can enable Direct Connected Hosted Connections for GovCloud, by leveraging the Equinix global network or in conjunction with the AWS Gateway network service. For additional details and best practices of Direct Connect for GovCloud, see the ECXF Documentation Center. Please note that the direct private connectivity of ITAR (International Arms Traffic Regulation) through AWS Direct Connect is only provided through SV5.

Source: [https://www.equinix.es/partners/AWS/]

b. Each AWS Direct Connect connection can be configured with one or more virtual interfaces. Virtual interfaces may be configured to access AWS services such as Amazon EC2 and Amazon S3 using public IP space, or resources in a VPC using private IP space. To access public resources in a remote Region, you must set up a public virtual interface and establish a Border Gateway Protocol (BGP) session. After you have created a public virtual interface and established a BGP session to it, your router learns the routes of the other public AWS Regions. You can create a Direct Connect gateway in any public Region. Use it to connect your AWS Direct Connect connection over a private virtual interface to VPCs in your account that are located in different Regions or to a transit gateway. Alternatively, you can create a public virtual interface for your AWS Direct Connect connection and then establish a VPN connection to your VPC in the remote Region.

If you're using AWS Direct Connect to access public AWS services, you must specify the public IPv4 prefixes or IPv6 prefixes to advertise over BGP. The following inbound routing policies apply:
• You must own the public prefixes and they must be registered as such in the appropriate regional internet registry.
• Traffic must be destined to Amazon public prefixes. Transitive routing between connections is not supported.
• AWS Direct Connect performs inbound packet filtering to validate that the source of the traffic originated from your advertised prefix.

The following outbound routing policies apply:

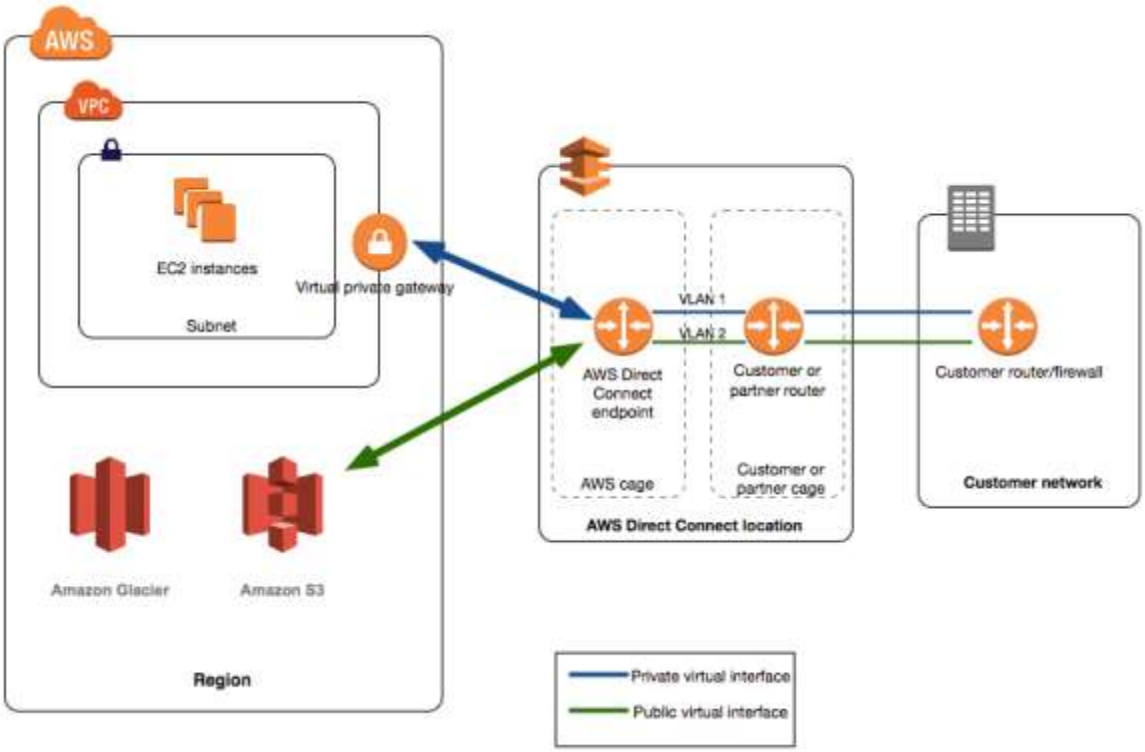
- ✓ AS_PATH is used to determine the routing path, and AWS Direct Connect is the preferred path for traffic sourced from Amazon. Only public ASNs are used internally for route selection.
- ✓ AWS Direct Connect advertises all local and remote AWS Region prefixes where available and includes on-net prefixes from other AWS non-Region points of presence (PoP) where available; for example, CloudFront and Route 53.
- ✓ AWS Direct Connect advertises prefixes with a minimum path length of 3.
- ✓ AWS Direct Connect advertises all public prefixes with the well-known NO_EXPORT BGP community.
- ✓ If you have multiple AWS Direct Connect connections, you can adjust the load-sharing of inbound traffic by advertising prefixes with similar path attributes.
- ✓ The prefixes advertised by AWS Direct Connect must not be advertised beyond the network boundaries of your connection. For example, these prefixes must not be included in any public internet routing table.

AWS Direct Connect supports local preference BGP community tags to help control the scope (Regional or global) and route preference of traffic on private virtual interfaces and transit virtual interfaces.

Source: [https://docs.aws.amazon.com/directconnect/latest/UserGuide/dc-ug.pdf]

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

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



The following are the key components that you use for AWS Direct Connect:

- Connections: Create a connection in an AWS Direct Connect location to establish a network connection from your premises to an AWS Region.
- Virtual interfaces: Create a virtual interface to enable access to AWS services. A public virtual interface enables access to public services, such as Amazon S3. A private virtual interface enables access to your VPC.
- Network Requirements: To use AWS Direct Connect in an AWS Direct Connect location, your network must meet one of the following conditions:
    - Your network is co-located with an existing AWS Direct Connect location.
    - You are working with an AWS Direct Connect partner who is a member of the AWS Partner Network (APN).
    - You are working with an independent service provider to connect to AWS Direct Connect.
    - In addition, your network must meet the following conditions:
        - Your network must use single-mode fiber with a 1000BASE-LX (1310 nm) transceiver for 1 gigabit Ethernet or a 10GBASE-LR (1310 nm) transceiver for 10 gigabit Ethernet.
        - Auto-negotiation for the port must be disabled. Port speed and full-duplex mode must be configured manually.
        - 802.1Q VLAN encapsulation must be supported across the entire connection, including intermediate devices.

- Your device must support Border Gateway Protocol (BGP) and BGP MD5 authentication.
- (Optional) You can configure Bidirectional Forwarding Detection (BFD) on your network. Asynchronous BFD is automatically enabled for AWS Direct Connect virtual interfaces, but does not take effect until you configure it on your router.

✓ AWS Direct Connect supports both the IPv4 and IPv6 communication protocols. IPv6 addresses provided by public AWS services are accessible through AWS Direct Connect public virtual interfaces.

✓ AWS Direct Connect supports an Ethernet frame size of 1522 or 9023 bytes (14 bytes Ethernet header + 4 bytes VLAN tag + 20 bytes for the IP datagram + 4 bytes FCS) at the link layer. You can set the MTU of your private virtual interfaces.

Source: [https://docs.aws.amazon.com/directconnect/latest/UserGuide/dc-ug.pdf]

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?

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.)

Solution:

Network Address Translation (NAT), developed by Cisco, is designed for IP address conservation. It enables private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network.

As part of this capability, NAT can be configured to advertise only one address for the entire network to the outside world. This provides additional security by effectively hiding the entire internal network behind that address. NAT offers the dual functions of security and address conservation and is typically implemented in remote-access environments.

a. You can use a NAT device 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.

- AWS offers two kinds of NAT devices—a NAT gateway or a NAT instance.
- NAT gateway: You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.
- NAT instance: You can use a network address translation (NAT) instance in a public subnet in your VPC to enable instances in the private subnet to initiate outbound IPv4 traffic to the Internet or other AWS services, but prevent the instances from receiving inbound traffic initiated by someone on the Internet.
- Using NAT for a virtual private subnet with the Amazon Direct Connect service:
- You can use the Amazon VPC console to create, view, and delete a NAT gateway. You can also use the Amazon VPC wizard to create a VPC with a public subnet, a private subnet, and a NAT gateway.
- When the database servers in a private subnet, you can set up security and routing so that the web servers can communicate with the database servers, but we can prevent the Internet from initiating connections with instances. When the traffic goes to the Internet, the source IP is replaced with the NAT's device address and similarly when traffic goes to the instances, the NAT device translates the address back to the instance's private IP address.
- As NAT causes loss of end-device to end-device IP traceability, I would not use it where I want to trace the IP Address of the parties communicating.

Source: [https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html]

b. If we pretend that we live in a simple world where each system only has 1 IP address, then a 'normal system' would be limited to an absolute maximum of $2^{16} =$ 65536 connections. Since 4,096 are reserved, so 65536-4096=**61440** can be maintained.

Source: [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?

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

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

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

Solution:

a.

I. The use of AWS Direct Connect with Amazon VPC requires the use of the Border Gateway Protocol (BGP) with an Autonomous System Number (ASN) and IP Prefixes.

II. Autonomous Systems are the unit of routing policy in the modern world of exterior routing, and are specifically applicable to protocols like EGP (Exterior Gateway Protocol, now at historical status.

III. An AS must be used for exchanging external routing information with other ASes through an exterior routing protocol.

IV. The current recommended exterior routing protocol is BGP, the Border Gateway Protocol.

V. Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet.

VI. The Border Gateway Protocol makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator and is involved in making core routing decisions. So, to use AWS Direct Connect with Amazon VPC, the Border Gateway Protocol is required.

Source:[https://aws.amazon.com/directconnect/faqs/] [https://en.wikipedia.org/wiki/Border_Gateway_Protocol] [http://www.ietf.org/rfc/rfc1930.txt]

b.

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.

Source: [http://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 over time, eventually dividing the responsibility for management to a registry for each of five regions of the world.
  - i) The African Network Information Center (AFRINIC) serves Africa.
  - ii) The American Registry for Internet Numbers (ARIN) serves Antarctica, Canada, parts of the Caribbean, and the United States.

iii) The Asia-Pacific Network Information Centre (APNIC) serves East Asia, Oceania, South Asia, and Southeast Asia.

iv) The Latin America and Caribbean Network Information Centre (LACNIC) serves most of the Caribbean and all of Latin America.

v) The Réseaux IP Européens Network Coordination Centre (RIPE NCC) serves Europe, Central Asia, Russia, and West Asia.

- ✓ To establish an ASN for your data center in Sapporo, Japan, I would go to Asia-Pacific Network Information Centre (APNIC). It provides numbers resource allocation and registration services that support the global operation of the internet. It is a nonprofit, membership-based organization whose members include Internet service providers, telecommunication providers, data centers, universities, banks, national Internet registries, and similar organizations that have their own networks.

Source: [https://en.wikipedia.org/wiki/Asia-Pacific_Network_Information_Centre]

d.

BGP helps routers decide how to send giant flows of data across the vast mesh of connections that make up the Internet. With infinite numbers of possible paths — some slow and meandering, others quick and direct — BGP gives routers the information they need to pick one, even though there is no overall map of the Internet and no authority charged with directing its traffic.

- ❖ The main reason BGP is "hijacked", 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.
- ❖ Also, BGP has security issues like Eavesdropping, Replay, Message Insertion, Message deletion, message modification and Man-In-The-Middle attacks and Denial-of-service.

The security problems can be addressed by:

- Acquiring cryptographic keys for identifying networks in cyberspace
- Secure-BGP: It is a comprehensive solution to BGP Security
- The Interdomain Route Validation (IRV) service is a receiver-driven protocol and associated architecture [Goodell et al. 2003]. Unlike S-BGP, IRV's operation is independent of the routing protocols.
- Secure origin BGP (soBGP) proposes an extension to BGP [Ng 2002]. soBGP adds small security enhancements to the existing BGP protocol. The primary mechanism of soBGP is the new SECURITY message type. The SECURITY message is used by BGP speakers to share certificates and attestations. The data of these messages are signed by the sender and allows the receiver to validate the public key bindings, policy, or routing data.
- Received information has data integrity if one can validate that it has not been modified in transit. If data integrity is not provided, an adversary may modify the information in any number of ways. For example, an adversary may alter the AS path so that data is routed across a subverted link. Source, or origin,

authentication is a subtly different property that guarantees the identity of the sending peer (e.g., the sending peer is in fact who he or she claims to be).

- Origin Authentication (OA) is a method of validating address ownership. It addresses what is potentially the most dangerous problem currently facing BGP, because of the protocol's inherent vulnerabilities. A misconfigured router that originates incorrect route information, or even information relating to an AS it does not own, can cause major black hole effects throughout the entire Internet

Source: [https://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/?utm_term=.997a3587f334]
[https://www.researchgate.net/publication/224092573_A_Survey_of_BGP_Security_Issues_and_Solutions (A Survey of BGP Security Issues and Solutions: TONI FARLEY, PATRICK MCDANIEL and KEVIN BUTLER AT&T Labs Research)]

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. Bernard, 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.)

Solution:

Yes, the dogs can provide this service of inter-connection. There are two dogs, Alpha and Beta, each having 3 disks attached. Each disk stores 7Gb of data. Considering that Alpha starts from data center 1 and goes to data center 2; Beta starts from data center 2 and goes to data center 1. So, Alpha has 3*7=21Gb of data attached to it and Beta has 3*7=21Gb of data attached.

Now, the dogs run at speed 18 km/hr and the distance between the data centers is 5.5 km; so time required (T) to cover that distance by Alpha= distance/speed=5.5/18=0.3 hrs=18 minutes =1080 seconds approximately.

Similarly, time required for Beta to cover the distance= 5.5/18=0.3hrs=18 minutes =1080 seconds approximately.

So, the data of 21 Gb (21000 Mb) can be transferred by Alpha to data center on the opposite side in 18 minutes. So, the speed in seconds is 21000/1080=19.44 Mbps.

Similarly, Beta can give data speed of 19.44 Mbps.

Now, comparing this with our data pipes, data pipes give a speed of 150 Mbps in each direction. So, the St. Bernard dogs would provide less efficiency as: 150/19.44=7.71.

The dogs are 7.71 times slower as compared to data pipes.

[This calculation is based on assumption that the dogs, Alpha and Beta will not take any break during their journey from data center 1 to data center 2 or data center 2 to data center 1 respectively. Also, I have assumed that they wont face any obstacles(physical path terrain hurdles). Moreover, security concerns are completely neglected for this solution]