CS 524 Introduction to Cloud Computing

Dharmit Viradia

Homework 3

Prof. Igor Faynberg

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?

Sol: Steps to calculate burst time are as follows:

1. A token is added to the bucket every seconds.
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. And if fewer than 'n' tokens are available then no tokens will be removed from the bucket.
4. Now, considering M is a maximum output rate and r is a token rate then Tmax (maximum burst time) will be: Tmax = b/(M-r).

2) Study the AWS Direct Connect service and answer the following questions:

a. 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 a good deal of 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. As you have noticed, the AWS Direct Connect service description refers to the IEEE standard 802.1q. Read this standard (available at http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf) 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."

Sol: AWS Direct Connect makes it easy to establish a dedicated network connection from premises to AWS. We can establish private connectivity between AWS and data center, office, co-location environment, which in many cases can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet based connections.

a. If I own a company with data center in 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.
   - Provides a flexible range of speeds (50, 100, 200, 300, 400, and 500 Megabits per second) with Virtual Connections (VCs) via Equinix Cloud Exchange.
   - Provides cross connections either 1 or 10 Gigabits per second connections.
   - Offers Amazon Direct Connect services covers more geographical locations than any other data center provider. AWS GovCloud is available in all U.S. AWS Direct Connect locations.
   - Offers latest technology capabilities and has the facility to migrate to hybrid cloud computing.

b. With AWS Direct Connect, you can establish 1 Gbps or 10 Gbps dedicated network connections between AWS and any of the AWS Direct Connect locations. A dedicated

connection can be partitioned into multiple logical connections by using industry standard 802.1QVLANs. In this way, you 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. You can choose a partner from the AWS Partner Network (APN) to integrate the AWS Direct Connect endpoint in an AWS Direct Connect location with your remote networks.

Finally, you may combine all these different options in any combination that make the most sense for your business and security policies. For example, you could attach a VPC to your existing data center 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.

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

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

Sol: AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1 gigabit or 10 gigabit Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. You can create virtual interfaces directly to the AWS cloud (for example, to Amazon EC2 and Amazon S3) and to Amazon VPC, bypassing Internet service providers in your network path. 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). You need the following information to complete the connection:

- A public or private ASN. If you are using a public ASN you must own it else if you are using a private ASN, it must be in the 65000 range.
- A new unused VLAN tag that you 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. You can advertise the default route via BGP).

The Virtual Private Gateway to connect:

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

- Open the AWS Direct Connect console.
- In the connection pane, select the connection to use, and then click Create Virtual Interface.
- In the Create a Virtual Interface pane, select Private.
- Under Define Your New Private Virtual Interface
    - o Enter a name for the virtual interface in the Interface Name field.
    - o In the Interface Owner, select the My AWS Account option if the virtual interface is for your AWS account ID.
    - o Select the virtual gateway to connect to, In the VGW list.
    - o In the VLAN # field, enter the ID number for your virtual local area network (VLAN); for example, a number between 1 and 4094.
    - o To have AWS generate your router IP address and Amazon IP address, select Auto-generate peer IPs.
    - o To specify these IP addresses yourself, clear the Auto-Generated peer IPs check box, and then in 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 Amazon Web Services.
    - o 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.
    - o 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 your 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, you 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)

4) 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.)

Sol: Network Address Translation (NAT) is a method of remapping one 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 an unique IP address to public network on the behalf of entire group of computers on private network.

a. 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, for software

updates) or other AWS services, but prevent 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 goes to the Internet, the source IP address is replaced with the NAT device's address and similarly, when response traffic goes to 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 here is no 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.

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

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

(Reference: Cloud Computing: Business Trends and Technologies)

5) Read RFC 1930 (http://www.ietf.org/rfc/rfc1930.txt) 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?

Sol: 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. Border Gateway Protocol is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the internet. BGP is used to communicate 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 which 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. 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. Yes, we can use our own ASN to connect to VPC 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.

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

c. Regional Internet Registry (RIR) is an organization that 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 my data center in Sapporo, Japan, I would go to Asia Pacific Network Information Centre (APNIC). APNIC provides number resource allocation and registration services that support the global operation of the Internet. It is a non-for-profit, membership-based organization whose members include Internet Service Providers, National Internet Registries, and similar organizations. The main functions of APNIC are: • allocating IPv4 and IPv6 address space, and Autonomous System Numbers, • maintaining the public WhoIs Database for the Asia Pacific region, • reverse DNS delegations, • 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/AsiaPacific_Network_Information_Centre, https://www.apnic.net/)

d. The challenge with BGP is that the protocol does not directly include security mechanisms and is based largely on trust between network operators that they will secure their systems correctly and not send incorrect data. Mistakes happen, though, and problems could arise if malicious attackers were to try to affect the routing tables used by BGP. There are several commonly used mechanisms for supporting secure and private communication, transaction protection and identity assertion and management. These include the so-called Internet PKI commonly used for secure web browsing but which can be used for other applications, PKI for e-mail, RPKI used by Regional Internet Registries to assert the holders of IP resources, and DNSSEC that 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.

6) 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.

Now, you retrain your company's two St. Bernard's, 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-Mbpsdata 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.)

Sol: 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 = 5500 m

Time taken by Dogs to travel to the data center
Time = Distance/Speed
= 5.5/18 km/hr
= 1099.8 sec

Time taken to transfer the data
Date Rate = Data/Time
= 21000*8/1010
= 168000/1099.8
= 152.755 Mbps

Hence the Bernard's Dogs can provide the service same as renting pipes for free.