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?

Ans: The token bucket is an algorithm used in packet-switched computer networks and telecommunication networks. It can be used to check that data transmissions, in the form of packets, conform to defined limits on bandwidth and burstiness (a measure of the unevenness or variations in the traffic flow). It can also be used as a scheduling algorithm to determine the timing of transmissions that will comply with the limits set for the bandwidth and burstiness: see network scheduler.

When a packet is to be checked for conformance to the limits, the bucket is inspected to see if it contains sufficient tokens at that time. If happens, then the number of tokens is removed and the packet is passed for transmission.

The basic steps to calculate the burst time are as follows:

1. A token is added to the bucket every 1/r seconds.

2. Bucket size (b bytes) means the bucket can hold at the most b tokens and if a token arrives when the bucket is full then that will be discarded.

3. If a packet of 'n' bytes arrives then 'n' tokens will be removed from the bucket and is sent to the network. And if fewer than 'n' tokens are available, then no tokens will be removed from the bucket.

4. Considering M is a maximum output rate and r is a token rate then maximum burst time(Tmax) will be:

Tmax = b / (M-r) if r < M

∞ otherwise

5. In the above equation, Tmax is the time for which the rate M is fully utilized. Therefore, the maximum burst time is **Tmax = b/(M-r)**.

(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.)

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."

Ans: 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 happen to own a company with a data center in Sapporo, Japan. I would choose to connect Equinix OS1, Osaka, Japan among other partners to connect this location to the AWS. As with Equinix data centers

• 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.

• It provides a flexible range of seeds with virtual connections via the Equinix Cloud Exchange.

• Offers facility to migrate to hybrid cloud computing.

QoS Guarantees:

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

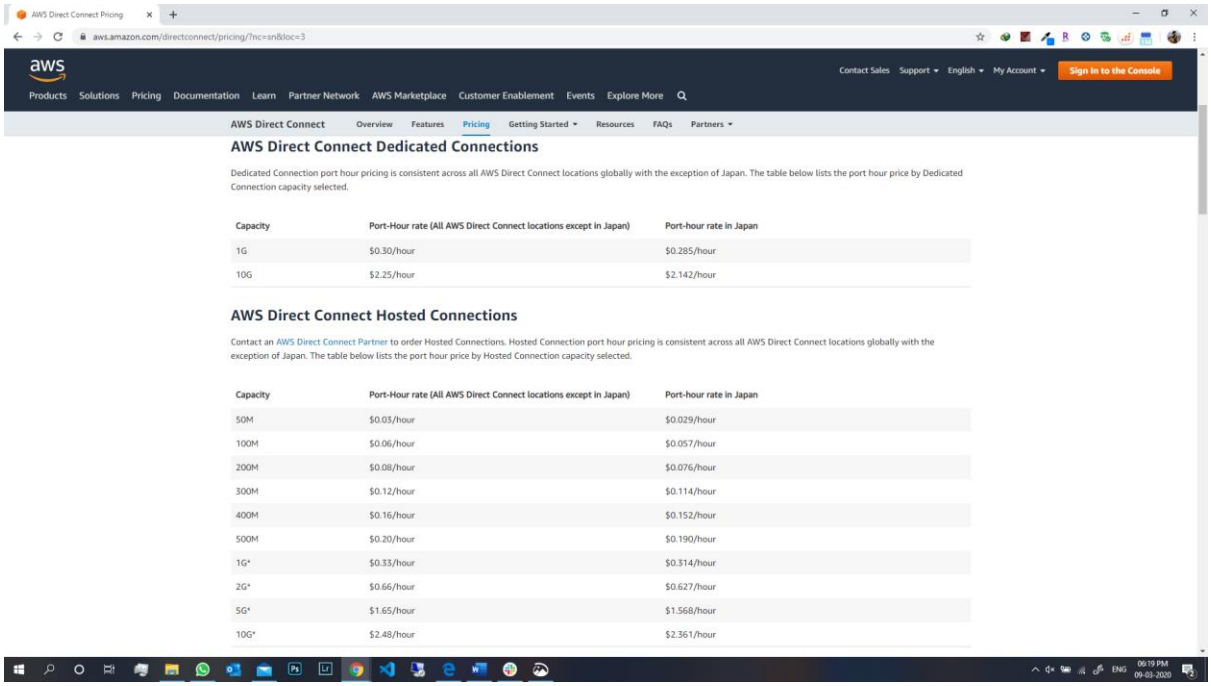
• Security - Each Equinix IBX data center utilizes an array of security equipment, techniques and procedures to control, monitor, and record access to the facility, including individual cages.

• High average uptime—Our IBX data centers boast an industry-leading track record of >99.99999%.

• Proven expertise—We can help you configure and support your high-power density deployments.

• Recovery – IBXflexTM Space provides operations centers and storage space when you need it. Equinix Smart HandsTM offers 24-hour access to qualified technical support—with Equinix, you can maintain your mission-critical operations and equipment under any circumstances.

• 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.



AWS Direct Connect Pricing

aws.amazon.com/directconnect/pricing/?nc=sn&loc=3

aws

Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer Enablement Events Explore More

Contact Sales Support English My Account Sign In to the Console

AWS Direct Connect Overview Features Pricing Getting Started Resources FAQs Partners

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

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

(Reference: https://aws.amazon.com/directconnect/pricing/?nc=sn&loc=3 & https://aws.amazon.com/directconnect/?nc=sn&loc=1)

b. With AWS Direct Connect, you can establish 10 Gbps dedicated network connections between AWS Direct Connect locations and AWS. A dedicated connection can be partitioned into multiple logical connections by using industry-standard 802.1QVLANs.This connection can be used to access public resources such as objects stored in Amazon Simple Storage Service.

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).

VPN connections have low to modest bandwidth requirements and can tolerate variability in internet-based connectivity.AWS direct connect uses dedicated, private network connections between intranet and Amazon VPC.

AWS will locate private IPs in the 169.x.x.x range for the BGP session and will advertise the VPC CIDR block over BGP.

(Reference: https://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).

Ans: AWS Direct Connect links the 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.

We can create virtual interfaces directly to the AWS cloud and Amazon VPC, bypassing Internet service providers in your network path. When you create a private virtual interface to a VPC you want to connect. This connection requires the use of the Border Gateway Protocol.

Details to get connection:

• A public or private ASN.If a user is using public ASN then he has to own it, if he is using ASN, then it must be in the 65000 range.

• A new unused VLAN tag that you select.

• The VPC Virtual Private Gateway id

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

• 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.

• Select the virtual gateway to connect to, In the VGW list.

• 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.

• To specify these IP addresses yourself, clear the Auto-Generated peer IPs checkbox, and then in the Your router peers 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.

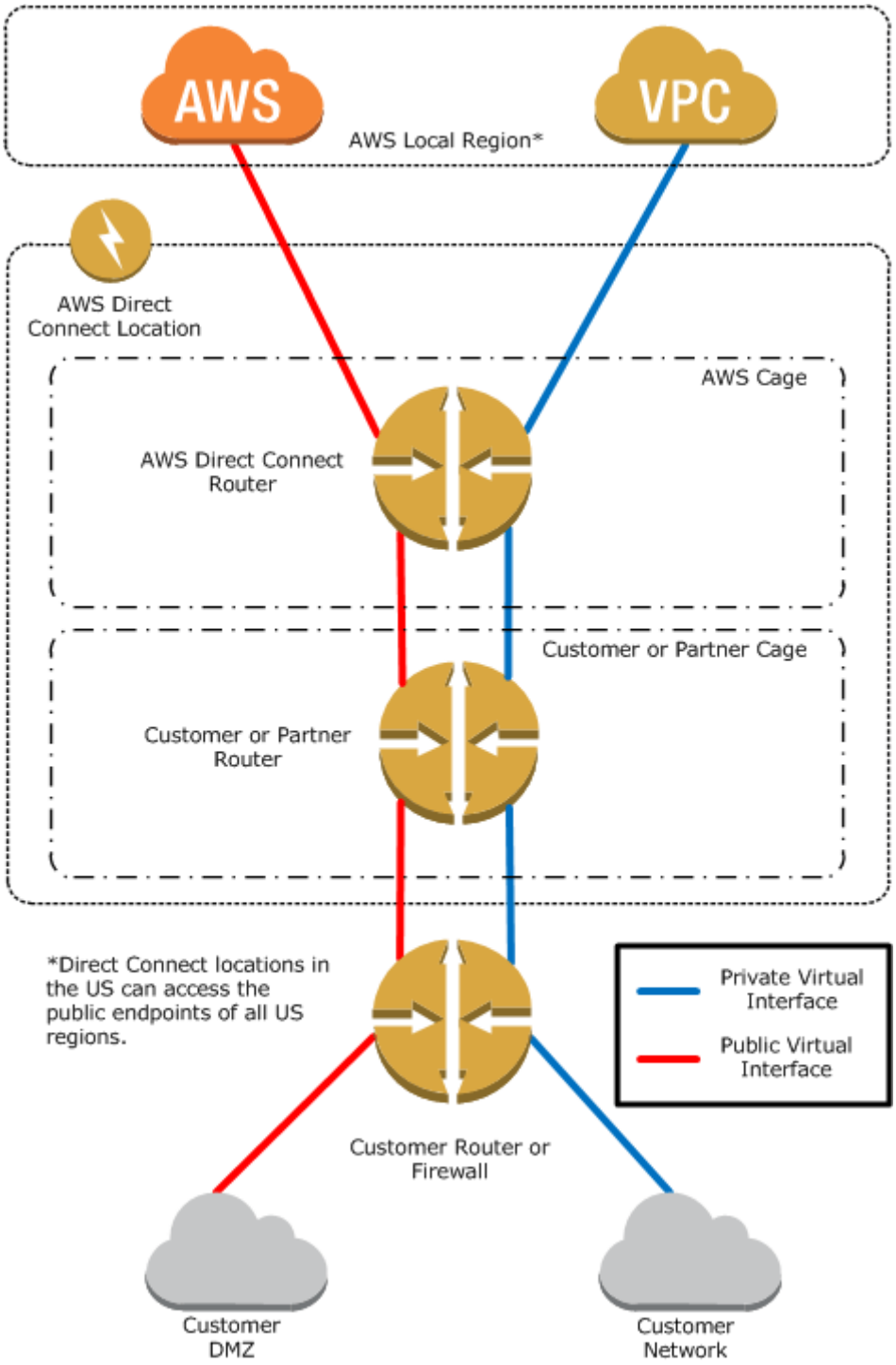
• In the BGP ASN filed, enter the Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your gateway; for example, a number between 1 and 65534.

• Select Auto-generate BGP key checkbox to have AWS generate one.

To provide your BGP key, clear the Auto-generate BGP key checkbox and then in the BGP Authorization key field, enter your BGP MD5 key.

Download your router configuration and configure the router.

AWS Direct Connect Interfaces with the network.



(References: https://datacenterrookie.wordpress.com/2017/03/03/direct-connect-to-the-aws-cloud/, https://aws.amazon.com/directconnect/, https://docs.aws.amazon.com/directconnect/latest/UserGuide & http://docs.aws.amazon.com/directconnect/latest/UserGuide/images/direct_connect_architecture.png)

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.)

Ans: Network address translation (**NAT**) is a method of remapping one 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. The technique was originally used as a shortcut to avoid the need to readdress every host when a network was moved. It has become a popular and essential tool in conserving global address space in the face of IPv4 address exhaustion. One Internet-routable IP address of a NAT gateway can be used for an entire private network.

a. NAT is used for a virtual private subnet with the Amazon Direct Connect Services to enable instances in a private subnet to connect to the internet. When traffic goes to the internet, the source IP address is replaced with the NAT device address, when response traffic goes to those instances, the NAT devices translate the address back to those instances private IP addresses.

When the user is working with instances, that require the use of static public IP address and when there is no Internet gateway to enable communications over the internet which includes VPC with a single private subnet and a virtual private gateway to enable communication with the network over an IPsec VPN tunnel.

(References: https://en.wikipedia.org/wiki/Network_address_translation, https://whatismyipaddress.com/nat , https://www.geeksforgeeks.org/computer-network-network-address-translation-nat/ & https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html)

b. The maximum number of connections that a single NAT box can maintain is 65536. But the first 4096 ports are reserved, the effective number of maximum connections that can be used are 65536-4096 is 61440.

(References: 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?

Ans:

a. 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 a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet. The protocol is classified as a path vector protocol. 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.

Border Gateway Protocol is used to communicate between two routing domains. Sending router decides on the shortest path to the destination based on the routing table lookup.

(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 is 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 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 numbers.

To establish an ASN for my data center in Sapporo, Japan, I would go to the Asia Pacific Network Information Centre (APNIC). APNIC provides the number of resource allocation and registration services that support the global operation of the Internet. It is a non-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 Whois Database which is public for the Asia Pacific region.

• Reverse DNS delegations.

(References: https://en.wikipedia.org/wiki/Regional_Internet_registry & https://en.wikipedia.org/wiki/AsiaPacific_Network_Information_Centre)

d. Below are three ways in which attackers can potentially abuse BGP.

- **BGP route manipulation**: A malicious device alters the content of the BGP table, preventing traffic from reaching the intended destination.
- **BGP route hijacking**: A rogue device maliciously announces a victim's prefixes to reroute traffic to or through itself, which otherwise would not happen. Rerouting traffic can cause instability in some networks with a sudden load increase. This allows attackers to access potentially unencrypted traffic to which they would otherwise not have access or use hijacked BGP to launch spam campaigns, bypassing IP blacklist mitigation.
- **BGP denial-of-service (DoS)**: A malicious device sends unexpected or undesirable BGP traffic to a victim, exhausting all resources and rendering the target system incapable of processing valid BGP traffic.

While some BGP incidents are intentional, others, such as BGP route leaks, may be caused by inadvertent misconfigurations within the operations of these large networks. Regardless of intent, they can render the internet vulnerable and unstable.

Mitigation of the Threats

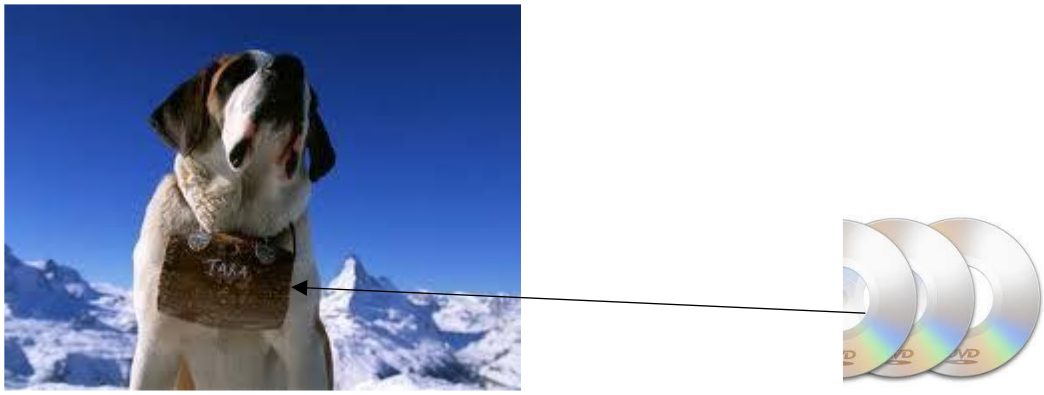
BGP incidents put the internet's stability at risk. For many internet providers, routing security only becomes a priority in the aftermath of an incident. However, long-term protection against BGP abuse requires organizations to implement security measures.

Fortunately, there is a silver lining. Given the dimension of the problem to be tackled, standardization bodies such as the Internet Engineering Task Force (IETF) and agencies such as the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS) are teaming up to provide a better set of security standards for BGP. Through this effort, the agencies have made available the Secure Inter-Domain Routing (SIDR) framework with a focus on the following three components: Resource Public Key Infrastructure (RPKI), BGP Origin Validation and BGP Path Validation (BGPSec).

This initiative is supplemented by enormous efforts to make BGP data available. Entities such as router equipment vendors, internet content and access providers, and transit networks are encouraged to share data to help solve this problem.

Organizations seeking to protect their networks from BGP internet routing attacks can leverage BGPSec, an extension of BGP that provides additional security. When used in conjunction with origin validation, it may prevent a variety of route hijacking attacks. The downside is that BGPSec can potentially result in more complexity in routing updates and may require more hardware to compute signatures — possibly a large infrastructural change with many unknowns for some operators. Security firm Team Cymru also developed a list of BGP templates to help organizations secure BGP on their routers.

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.)

Ans: Given,

Each disk stores 7Gb of data = 7,000 megabytes = 7,000,000 bytes (as per the given conversion in question) = 56,000,000 bits (1 Byte = 8 bits)

Distance between data centers = 5.5 Km

The speed at which Alpha & Beta can run = 18 Km/h

The time taken by Alpha and Beta to reach their destination = 5.5 / 18 = 0.3056 hr = 18.36 min

So, the other end of the data center will be receiving 7Gb of data every 18.36 min.

To ensure the link speed is 150 Mbps, the amount that needs to be received in an hour = 150 * 60 * 60 = 540,000 Megabits = 67,500 Megabytes.

Since the amount of data supplied by Alpha and Beta surpasses the amount of data required to maintain the link speed of 150 Mbps, we can say the St. Bernards can be successfully deployed to achieve the situation.