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?

Answer:

The tokens are represented a unit of byte or a single packet of established size and are then added at a fixed rate. An incoming packet must have sufficient tokens before admission into the network. Token rate regulates transfer of packets and if sufficient tokens are available packets enter network without delay. Token bucket could be used for controlling when you want to limit the rate of something. The token bucket constraints the traffic from a source to be limited to b + r * t bits in an interval of length t. It can be used to check the transmissions of data in the form of packets conform to defined limits on burstiness and transmission capacity. To understand it can be put as:

- A token is added to bucket r tokens/ sec.
- The bucket can hold b tokens at maximum and if bucket is full it removes token.
- The packets coming through n bytes placed in token wait and, tokens are removed from the bucket which is sent to the network. If less tokens are available none of the tokens are removed from the bucket which the packet is considered to be radical.

It is good for traffic shaper, traffic policer and traffic marker.

The equation base on the data input, after time T, data output should equal to data input i.e.

$b + r * T = M;$

$T = b / (M-r)$

It is the maximum burst time i.e. time for which the rate M is thoroughly utilized. In the above formula, r is subtracted from M to calculate the maximum burst time. The reason for this subtraction is, new tokens are added at the rate of r while transmission happens at maximum transmission rate M. (En.wikipedia.org. 2020. Token Bucket)

2. 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."

a. Answer:

AWS Direct Connect is a cloud service that deals with solving of problem which makes it easy to establish a dedicated network connection from premises to AWS. It helps establish a committed network connection between the network and one of the AWS Direct Connect location. Working with an APN partner has many benefits such as it would help grow and scale business on AWS and also fast track the journey to the cloud making a favorable condition for all the AWS will or has to offer.

Since we know that AWS Direct Connect Partners provides help to establish connectivity between AWS Direct Connect choosing a ideal company is an important aspect. Looking through the AWS Direct Connect Partners by Direct Connect location in Asia in Asia Pacific (Tokyo) as the location of my company is in Sapporo, Japan; choosing Equinix Interconnection between others would be beneficial for my company as it provides:

Approved for Hosted Connections of capacities from 50Mbps to 10Gbps (network links used for capacities from 1Gbps to 10Gbps require additional monitoring) that gives flexible range of speeds with Connections via Equinix Cloud Exchange. It offers various options for high performance, private access to AWS Direct Connect covering the most market than any other data center provider, also offering the latest technology capabilities and has the facility to migrate to hybrid cloud computing.

AWS Direct Connect pricing is pay only for what you use and there is no minimum fee.

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

Table: Lists the port hour price by Direct 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.

Table: Lists the port hour price by Hosted Connection capacity selected.

(KaZaA, Direct Connect, eDonkey, bitTorrent a další: průvodce výměnou souborů přes Internet. (2004))

The **QoS** guarantees:

-> **Security:** Equinix IBX data center utilizes an array of security equipment, procedures to control, monitor, and record access to facilitate, various techniques including individual cages.

-> **Certifications:** Equinix data centers are certified that meets the demanding and rigorous energy management standards that enable smooth and efficient operations. Various certification is given and according to certification or area you can find the required certificates like, FISC (Security

Guidelines (Japan) The Center for Financial Industry Information Systems), ISO27001, PCI DSS, SOC 1, SOC 2. That can help configure and support high- power density deployments.

-> **Green by Design:** Build and operate data centers with high energy efficiency standards and a long-term goal of using 100% clean and renewable energy. Recently 92% renewable energy coverage globally in 2018 up from 77% in 2017. But as leaders in data center sustainability Equinix are taking steps to minimize our carbon footprint and reduce our energy consumption.

-> **Power:** Our IBX data centers boast an industry-leading track record of >99.99999%. 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.

-> **Cooling:** Equipment's operating at its peak, each data center houses a multicomponent temperature control system are running 24/7. Robust heating, ventilation and air conditioning (HVAC) systems, Equinix IBX data centers exceed the requirements of even the most power-hungry deployments. We provide 14M+ ft^2 of data center space across 40 markets in 21 countries on 5 continents. 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. (Data Center Design. (n.d.)).

b. Answer:

Between the allocated network connections AWS and any of the AWS Direct Connect locations we can set up 1 Gbps or 10 Gbps with AWS Direct Connect. A committed connection can be partitioned into multiple logical connections by using industry standard 802.1QVLANs which is the networking standard that supports virtual LANs (VLANs) on an IEEE 802.3 Ethernet network. Since we are using the same connection and this method can access public resources as in object stored in Amazon Simple Storage Service (Amazon S3) that uses public IP address space, and private resources such as Amazon EC2 instances that are running within a VPC using private IP space and all of this while maintaining network separation between the public and private environments. Selecting a partner from the AWS Partner Network (APN) to merge the AWS Direct Connect endpoint in an AWS Direct Connect location with the company's remote networks. Eventually combining all these various options in any combination that make the most sense for the business and security policies.

As an example, we 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 that will advertise the VPC CIDR block over BGP. We can advertise the default route via BGP. AWS Direct Connect does not involve the Internet, instead it uses dedicate, private network connections between your intranet and Amazon VPC. 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.
(VPC: Validación periódica de la colegiación. (2016).
(AWS Direct Connect - docs.aws.amazon.com. (n.d)).
(AWS VPC Connectivity-d1.awsstatic.com. (n.d)).

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

Answer:

AWS Direct Connect can be used to establish a private virtual interface from any on premise network directly to the Amazon VPC providing with a private, high bandwidth network connection between the network and the VPC. AWS Direct Connect also makes it easy to establish a dedicated connection from an on-premises network to Amazon VPC. The use of AWS Direct Connect, we can establish private connectivity between AWS and data center, office, or colocation environment. AWS Direct Connect links directly to the AWS cloud such as Amazon EC2 and to Amazon VPC bypassing ISP (Internet Service Provider) in the network path. Many of the virtual interfaces, we can even establish private connectivity to multiple VPCs while maintaining network isolation.

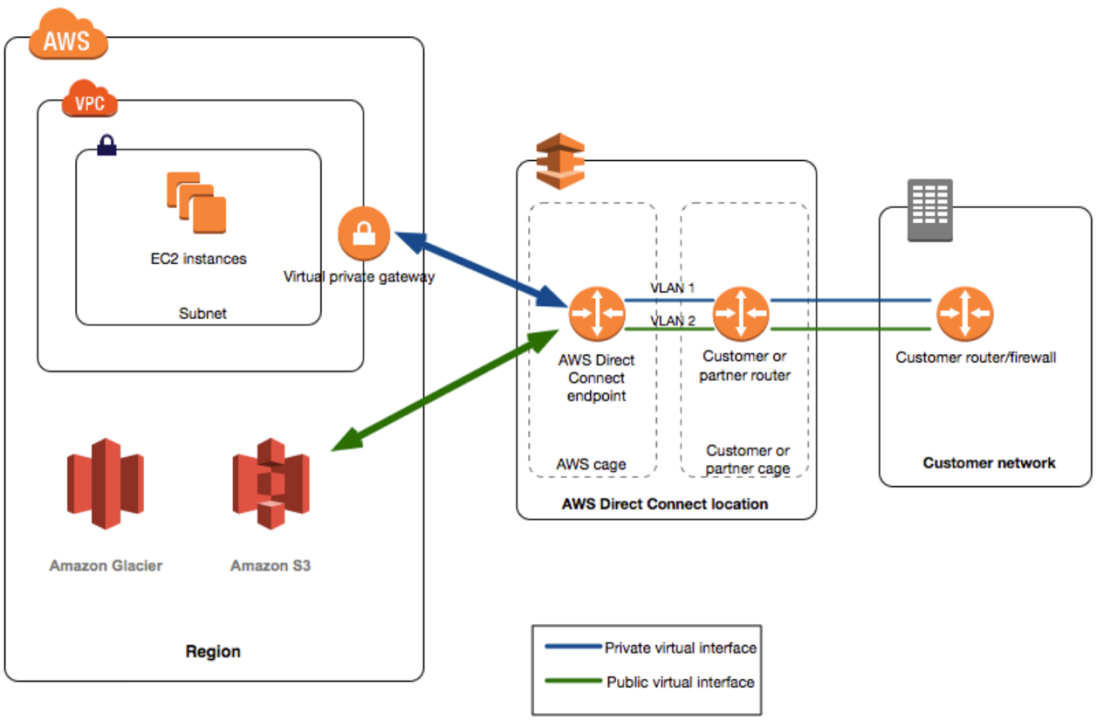

Fig: How AWS Direct Connect interfaces with the network

To create a virtual interface directly to the AWS cloud and to Amazon VPC, bypassing internet service provider in our network path. When creating a private virtual interface to a VPC we would need a private virtual interface for each VPC we would want to connect to, and this connection requires the use of Border Gateway Protocol (BGP). Public or private ASN and if we are using the public ASN we must own it otherwise when using the private it must be of range 65000 range, new and not used VLAN tag we selected and Virtual Private Gateway (VPG) id allocating private IPs by AWS in the 169.x.x.x range for the BGP session and will advertise the VPC CIDR block over BGP advertising the detail route through BGP. Following the above information, we can complete the connection. Hosted virtual interface works the same as a standard virtual interface and can connect to public resources or a VPC. A connection of less than 1 Gbps supports only one virtual interface. For creating a virtual interface we must specify the account and when an AWS account is choses that is not the account of themselves following rules will be applied:

- Private VIFs and transit VIFs the account applies to the virtual interface and the virtual private gateway or Direct Connect gateway destination.

- Public VIFs the account is used for virtual interface billing, the resource owner at AWS Direct Connect data transfer rate the Data Transfer Out (DTO) usage is metered to.

To create a virtual private gateway and attach it to your VPC

1. In the navigation pane, choose Virtual Private Gateways, Create Virtual Private Gateway.
2. (Optional) Enter a name for your virtual private gateway. Doing so creates a tag with a key of Name and the value that you specify.
3. For ASN, leave the default selection to use the default Amazon ASN. Otherwise, choose Custom ASN and enter a value. For a 16-bit ASN, the value must be in the 64512 to 65534 range. For a 32-bit ASN, the value must be in the 4200000000 to 4294967294 range.
4. Choose Create Virtual Private Gateway.
5. Select the virtual private gateway that you created, and then choose Actions, Attach to VPC.
6. Select your VPC from the list and choose Yes, Attach.

(docs.aws.amazon.com)

(KaZaA, DirectConnect, eDonkey, bitTorrent a další: průvodce výměnou souborů přes Internet. (2004)).

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.)

a. Answer:

Before talking about the use of NAT for virtual private subnet first we must know what NAT means, to simply put it NAT is the process where a network device most probably a firewall assigns a public address to a computer or many computers inside a private network so that it limits the number of public IP addresses an organization uses for security as well as economical purpose. NAT can be used to enable instances in a private subnet to connect to the internet or other AWS services while preventing the internet from initiating connections with the instances. Using the

NAT for virtual private subnet with the Amazon Direct Connect Services to enable instances in a private subnet to connect to the Internet or other AWS services preventing the Internet from initiating connections with instances. The main route table sends internet traffic from the instances in the private subnet to the NAT gateway and then the NAT gateway sends the traffic to the internet gateway using the NAT gateway's Elastic IP address as the source IP address. If a NAT gateway is not needed, we can delete it and deleting a NAT gateway disassociates its Elastic IP address also not releasing the address from the account it was created from.

For more than 55,000 continuous connections, also for the destination IP address, the destination port, or the protocol (TCP/UDP/ICMP) changes, we can create an additional 55,000 connections but there would be an increased chance of connection errors due to port allocation errors. Also if 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. (VPC: Validación periódica de la colegiación. (2016)).

b. Answer:

The maximum number of connections that a single NAT box can maintain is 2^{16} that is 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 that is 61440.

(Faynberg, I., Lu, H.-L., & Skuler, D. (2016)).

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:

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

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

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

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

1. Answer

Border Gateway Protocol (BGP) determines the route that is most suitable with the help of given information collected and an organization's routing policy that is based on cost, reliability, speed, and others. BGP is designed to exchange routing and reachability information between autonomous systems on the Internet. BGP enables sending router decides on the shortest path to the destination based on the routing table lookup which was previously obtained from the nearby domains as it is used to communicate between two routing domains so as to exchange routes from VPC to private network and followingly update it. Configurable Private Autonomous System Number (ASN), since this allows customers to set the ASN on the Amazon side of the BGP session for private VIFs on any newly created Direct Connect Gateway use of AWS Direct Connect with Amazon VPC the BGP is required.

(KaZaA, DirectConnect, eDonkey, bitTorrent a další: průvodce výměnou souborů přes Internet. (2004)).

(Leyes, Z. (2015, September 2)).

2.Answer

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 number between 64512 to 65535 range. Autonomous System numbers are used for identifying networks that present a clearly defined external routing policy to the Internet. (KaZaA, DirectConnect, eDonkey, bitTorrent a další: průvodce výměnou souborů přes Internet. (2004)).

3. Answer

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.

For establishing an ASN for my data center in Sapporo, Japan, I would be going to 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.
(whatismyipaddress.com/rir)

4. Answer

Since security was not kept in mind while designing the Border Gateway Protocol (BGP) which could lead to criminal individuals and governments can and do exploit, causing varying degrees of damage.

One type of BGP attack is route hijacking, caused by someone using BGP to announce illegitimate routes, and a new kind of BGP route hijack attack has come to the forward as a man-in-the-middle attack.

The Internet Engineering Task Force (IETF) has undertaken two efforts to fix BGP security issues over the years, Routing Policy System Working Group (RPSL) and Secure Inter-Domain Routing (SIDR), but both have problems that have impeded their success.

Routing Policy System Working Group (RPSL): - which in turn standardized a language called Routing Policy Specification Language (RPSL), and a security model (RP-SEC).

Secure Inter-Domain Routing (SIDR): - It can check the security credentials in-band as BGP routes are exchanged (BGPSEC).

The first step toward better BGP security has been a new system of secure cryptographic keys for networks, allowing them to authenticate their identities in cyberspace and make clear what networks they ordinarily handle traffic for.

(Quick fix for an early Internet problem lives on a quarter-century later. (n.d)).

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. (See the picture below.)

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-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.)

Answer:

The data centers are 5.5km away and need 150 Mbps (megabits per second) data pipes, one in each direction.

Can we use the dogs?

We know that 1GB = 8000 megabits

7 GB = 56000 megabits

Therefore, 1 dog can carry 56000 * 3 = 168000 megabits

Speed of dog is 18 km/hr. which means that to cover 5.5km it will take:

5.5/18 = .306 hrs. = 1101.6 secs

In 1 sec the dog will be able to carry 168000/1101.6 = 152.6 megabits of data

Therefore, the speed of data transmission by dogs is 152.6 Mbps which is more than our desired speed 150 Mbps. Which means we CAN use the dogs to carry data.

However, we will also have to train the dogs to bite anyone who tries to take the discs; security is important. There are also security concerns if we use dogs as it carries sensitive organization data. Data transmitted must adhere to encryption protocols and rules about how it must be accessed and utilized, helping from data breach that could hence ruin the organization. True connectivity is much more than just simply linking one location to another it achieves a many to many connections that allows multiple entities to communicate, transfer data while also sharing resources. Considering this there are 2 choices at hand either to build a physical network or to rent pipes. The appropriate choice here depends on the context, if the two data centers we are developing are temporary and may or may not be there for a long term service, than it would not be economically sensible to build a new physical server although we can have reliable service in our hands. But we would also like to consider the maintenance cost of the network. It is pretty expensive and also if there is poor cable deployment is more than just messy to look at it can restrict airflow, preventing hot air from being expelled properly and blocking cool air from coming in. Over time, cable-related air damming can cause equipment to overheat and fail, resulting in costly downtime. On the contrary, renting seems to be more promising in such cases where we only pay for time used for the services provided by the administrator. Although expensive this option offers better security and lower latency.

(wwt.com. (n.d.))

(Banta, T. (n.d.)).

Reference

En.wikipedia.org. 2020. Token Bucket. [online] Available at:

<https://en.wikipedia.org/wiki/Token_bucket> [Accessed 10 March 2020].

KaZaA, Direct Connect, eDonkey, bitTorrent a další: průvodce výměnou souborů přes Internet.

(2004). Retrieved from https://aws.amazon.com/directconnect

(KaZaA, Direct Connect, eDonkey, bitTorrent a další: průvodce výměnou souborů přes Internet.

(2004)) Retrieved from https://aws.amazon.com/directconnect/pricing/

Data Center Design. (n.d.). Retrieved from https://www.equinix.com/data-centers/design/

VPC: Validación periódica de la colegiación. (2016). Retrieved from

https://aws.amazon.com/vpc/faqs/)

AWS Direct Connect - docs.aws.amazon.com. (n.d.). Retrieved from

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

AWS VPC Connectivity-d1.awsstatic.com. (n.d).

(n.d) Retrieved from https://d1.awsstatic.com/whitepapers/aws-amazon-vpc-connectivity-

options.pdf

(n.d) Retrieved from https://docs.aws.amazon.com/directconnect/latest/UserGuide/dc-

ug.pdf#WorkingWithConnections

KaZaA, DirectConnect, eDonkey, bitTorrent a další: průvodce výměnou souborů přes Internet.

(2004). Retrieved from https://aws.amazon.com/directconnect/#:~:text=You can use AWS

Direct, your network and your VPC.)

Faynberg, I., Lu, H.-L., & Skuler, D. (2016). Cloud computing business trends and technologies. Chichester, West Sussex: Wiley.

VPC: Validación periódica de la colegiación. (2016). Retrieved from https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html)

Leyes, Z. (2015, September 2). What is BGP: Border Gateway Protocol Explained. Retrieved from https://www.imperva.com/blog/bgp-routing-explained/

(n.d) Retrieved from https://whatismyipaddress.com/rir)

Quick fix for an early Internet problem lives on a quarter-century later. (n.d.). Retrieved from https://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/?utm_term=.2d4b15610580

(n.d) Retrieved from https://www.wwt.com/article/the-data-centers-are-talking-how-interconnected-data-centers-speed-up-digital-transformation

Banta, T. (n.d.). Data Center Interconnect: A Comprehensive Guide. Retrieved from https://www.vxchnge.com/blog/data-center-interconnect