CS 524 Homework #3

Due: March 17, 2019

This homework contains both technical and business-related problems, for the total of **100** points. Note that Problem 3 requires a good deal of a self-study. To this end, consider it a typical every-day problem you would need to solve if you worked as a product manager in a large company or ran a start-up company yourself.

Please complete reading Chapter 4

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*?

   Answer: The maximum burst time T is:
   T = b/ (M-r) ; if r<M
   T = ∞ ; otherwise

2. **(60 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 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.)

      Answer: If I own a company with a data center in Sapporo, Japan then I will choose Equinox OS1 or EquinoxTY for AWS data center to connect this location to the Amazon service.
      The price of Equinix OS1 to/from Asia Pacific (Tokyo) Region is $ 0.0491 per GB.
      Existing QoS frameworks: media streaming
      1. End to End(integration principle)
      2. Declarative
      3. Types of requirements
         - Flow synchronisation-an analog to consistency
         - Flow performance
         - Level of service(deterministic, predictive, best-effort)
         - Management policy (trade-off between mediaquality and bandwidth)
         - Cost of service

      Mechanisms to achieve QoS:

- QoS mapping to underlying services (Threadpriorities, etc.)
- Admission Testing
- Resource reservation protocol

Existing Qos frameworks: network communication

1. Approaches
   - intServ: reservation of resources, RSVP (RFC 2205)
   - diffServ: priorities based on the type of traffic, implemented as Differentiated Services Field (DSField) in the IPv4 and IPv6 Headers (RFC 2474)
2. QoS isn't widely used: only used in some enterprise networks, not on Internet, supported by some routers.
3. Problems with internet QoS
   - Hard to support reservation in high-volume routers for thousands of concurrent sessions
   - Encrypted traffic cannot be inspected
   - Ability to abuse QoS policies by both users and providers
4. It is argued that increasing internet bandwidth is a better way to meet users' quality expectations instead of employing some form of QoS.
   Types of Quality (QoS dimensions)
   1. Performance: response time, mean throughput
   2. Quality of result set: data "freshness", correctness ,amount of data returned
   3. Economic factors of query execution – especially important for a scalable utility service.

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."

Answer:

- 802.1Q adds a 32-bit field between the source MAC address and the EtherType fields of the original frame. The minimum frame size is left unchanged at 64 bytes. The maximum frame size is extended from 1,518 bytes to 1,522 bytes. Two bytes are used for the tag protocol identifier (TPID), the other two bytes for tag control information (TCI). The TCI field is further divided into PCP, DEI, and VID.
- In accordance with the IEEE 801.q specification, Virtual I/O Server administrators can instruct the Shared Ethernet Adapter to inspect bridged VLAN-tagged traffic for the VLAN priority field in the VLAN header. The 3-bit VLAN priority field allows each individual packet to be prioritized with a value from 0 to 7 to distinguish more important traffic from less important traffic. More important traffic is sent preferentially and uses more Virtual I/O Server bandwidth than less important traffic.

- Shared Ethernet Adapters, in Virtual I/O Server Version 1.4 or later, support GARP VLAN Registration Protocol (GVRP), which is based on Generic Attribute Registration Protocol (GARP). GVRP allows for the dynamic registration of VLANs over networks, which can reduce the number of errors in the configuration of a large network. By propagating registration across the network through the transmission of Bridge Protocol Data Units (BPDUs), devices on the network have accurate knowledge of the bridged VLANs configured on the network.
- When GVRP is enabled, communication travels one way, from the Shared Ethernet Adapter to the switch. The Shared Ethernet Adapter notifies the switch which VLANs can communicate with the network. The Shared Ethernet Adapter does not configure VLANs to communicate with the network based on information received from the switch. Rather, the configuration of VLANs that communicate with the network is statically determined by the virtual Ethernet adapter configuration settings.

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

   Answer:

- 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.
- You can use an AWS Direct Connect gateway to connect your AWS Direct Connect connection over a private virtual interface to one or more VPCs in your account that are located in the same or different Regions. You associate a Direct Connect gateway with the virtual private gateway for the VPC.
- Usually a private Autonomous System Number (ASN) is needed. Then, create a virtual private gateway and attach it to your VPC which enables access to network from VPC. The virtual private gateway is the VPN concentrator on the Amazon side of the VPN connection.

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?

      Answer:

- A virtual private gateway enables communication with your own system network over an IPsec VPN tunnel and extend network into the cloud and furthermore specifically get to the Internet from your VPC. It additionally enables to run a multi-layered application with a versatile web front end in an open (public) subnet, and to house

information in a private subnet that is associated with network by an IPsec VPN association.

- In some case, virtual private subnet has some drawbacks compared with public subnet. The instances in the public subnet can receive inbound traffic directly from the Internet, however the instances in the private subnet can't. The instances in the public subnet can send outbound traffic directly to the Internet, whereas the instances in the private subnet can't.

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.)

Answer:

- A single listening port can accept more than one connection simultaneously. There is a '64K' limit that is often cited, but that is per client per server port, and needs clarifying. Each TCP/IP packet has basically four fields for addressing; these are:
  source_ip source_port destination_ip destination_port
  < client > < server >
- Inside the TCP stack, these four fields are used as a compound key to match up packetsto connections (e.g. file descriptors).If a client has many connections to the same port on the same destination, then three of those fields will be the same - only source_portvaries to differentiate the different connections. Ports are 16-bit numbers, therefore the maximum number of connections.
- If a client has many connections to the same port on the same destination, then three of those fields will be the same - only source_portvaries to differentiate the different connections. Ports are 16-bit numbers, therefore the maximum number of connections any given client can have to any given host port is 64K. However, multiple clients can each have up to 64K connections to some server's port, and if the server has multiple ports or either is multi-homed then you can multiply that further.

5. (**10 points)** 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?

      Answer: First, the AWS Direct Connect with VPC need provide a private Autonomous System Number (ASN). Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet.

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

      Answer: Yes, but we need to follow condition required. 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 65534.

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

      Answer: Asia-Pacific Network Information Centre (APNIC) for Asia, Australia, New Zealand, and neighboring countries.