CIS 508 (Spring 2014) Assignment 3

Name:

Masdar Email Account:

Deadline: **14 Apr 2014, 11:59pm (Late submissions of assignments will not be marked)**

Submission Instructions:

1. Fill in this document
2. Save as a pdf file, with filename as “cis508-2014-asg3-[MasdarEmailAccount].pdf” (replace [MasdarEmailAccount] by your own Masdar Email Account)
3. Send as an attachment to sidckchau@gmail.com, with email subject as “[CIS 508] Assignment 3 (2014)” before the above deadline

Questions:

Part 1: TCP

1. Consider that only a single TCP (Reno) connection uses one 10Mbps link which does not buffer any data. Suppose that this link is the only congested link between the sending and receiving hosts. Assume that the TCP sender has a huge file to send to the receiver, and the receiver's receive buffer is much larger than the congestion window. We also make the following assumptions: each TCP segment size is 1,500 bytes; the two-way propagation delay of this connection is 100 msec; and this TCP connection is always in congestion avoidance phase, that is, ignore slow start.

- What is the maximum window size (in segments) that this TCP connection can achieve? (1 Mark)

873 segments

- What is the average window size (in segments) and average throughput (in bps) of this TCP connection? (1 Mark)

Average window size: 654 segments
Average throughput: 78480000 bps

- How long would it take for this TCP connection to reach its maximum window again after recovering from a packet loss? (1 Mark)

Time = Max Window Size/2 * propagation delay
So time = 43.7 seconds

Part 2: BGP

BGP is highly vulnerable to many kinds of (unintentional or intentional) misconfigurations.

2. On February 24, 2008, Pakistan government originally intended block Youtube access within Pakistan only using BGP, but eventually took down Youtube globally. Describe how incident happened. Why is such a vulnerability of BGP? How can we prevent this incident in the future? (2 marks)

#1 Pakistan Telecom posted through BGP protocol a redirect for Youtube's IP address, which is provided by Hong Kong Internet Service Provider and distributed to other ISPs around the world. With the propagation effect of BGP, the Youtube's IP address then got hijacked.

#2 Because BGP is a policy-based protocol, each router knows little about network topology. Each router chooses the best next-hops for each destination, and then broadcast their choices. Once an IP is hijacked, it will spread through the whole Internet pretty soon.

#3 Peers don't route-filter each other;
No trust anchors built into the allocation/routing system from the start;
Add detection system into BGP.

Part 3: Software-defined Networking

3. What is OpenFlow? How can OpenFlow realize the vision of software-defined networking? Describe the status quo and future developments of OpenFlow. (3 Marks)

#1 OpenFlow is a communication protocol that gives access to the forwarding plane (most commonly, a table used by router to determine destination) of a network switch or router over the network.

#2 OpenFlow allows direct access to and manipulation of the forwarding plane of network devices such as switches and routers, both physical and virtual (hypervisor-based).

#3 Status quo:

The 1.1 version of OpenFlow was released on Feb. 28, 2011. The current version is 1.4.

Future development:

Trends such as user mobility, server virtualization, IT-as-a-Service, andneed rapidly to respond to changing business conditions place significant demands on the network—demands that today's conventional network architectures can't handle. Software-Defined Networking provides a new, dynamic network architecture that transforms traditional network backbones into rich service-delivery platforms.

The future of networking will rely more and more on software. Implementations of SDN like OpenFlow would transform today's static networks into flexible, programmable platforms with high intelligence, scalability and secuity.