CSc8220: Assignment 2

Due at 12:30pm, Mar. 6

Part I

1. What are the differences between message confidentiality and message Integrity? Can you have confidentiality without integrity? Can you have integrity without confidentiality? Justify your answer.

2. What does it mean for a signed document to be verifiable and non-forgeable?

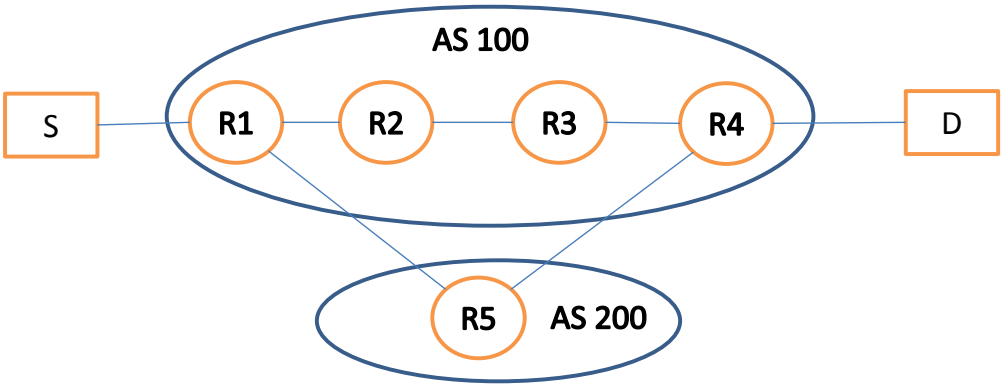
3. Suppose Alice wants to send an email to Bob. Bob has a public-private key pair (K_B^+, K_B^-), and Alice has Bob's certificate. But Alice does not have a public, private key pair. Alice and Bob (and the entire world) share the same hash function H(.).
    a. In this situation, is it possible to design a scheme so that Bob can verify that Alice created the message? If so, show how with a block diagram for Alice and Bob.
    b. Is it possible to design a scheme that provides confidentiality for sending the message from Alice to Bob? If so, show how with a block diagram for Alice and Bob.

4. Design a NACK-only Transfer Protocol (NTCP)

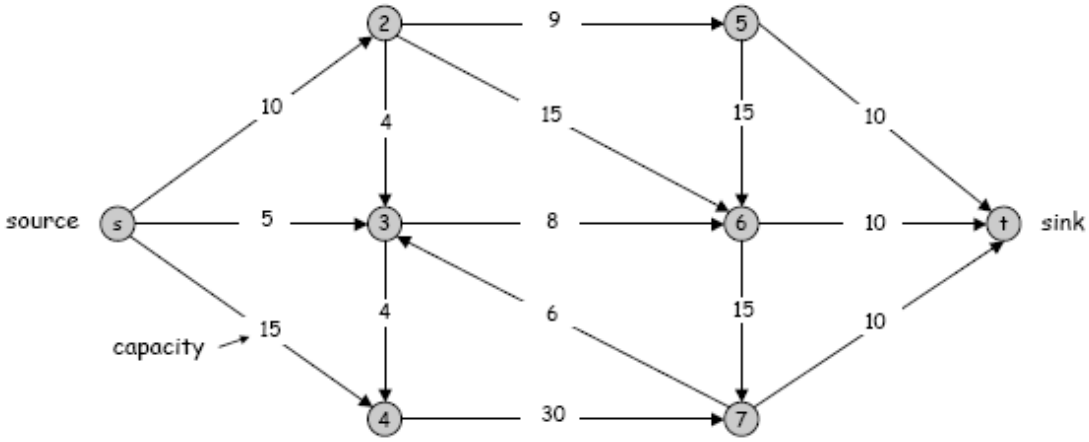
In HW1, you designed a reliable data transfer protocol that only uses negative acknowledgements (NACK), namely NTCP. The sender operates in a selective repeat fashion which an infinite window size (you may assume an infinitely large sequence number space if necessary), and only retransmits a packet when it receives a NACK from the receiver. The channel may lose or corrupt message and the delays are variable and unknown. Answer the following questions.

a. Would sequence numbers be necessary in this protocol?
b. Would a timer be necessary or advisable in this protocol? If so, would it be preferable to have the timer at the sender or receiver?
c. Describe the operation of a NACK-Only receiver that would operate with this sender. If there are scenarios (no matter how unlikely) that your receiver would fail to operate reliably, identify these scenarios.

5. In the following figure, R1, R2, R3, R4 are routers in AS100 and R5 is one router in AS200. If the shortest path routing algorithm is applied, what is the path from S to D. Explain how BGP would route data from S to D.

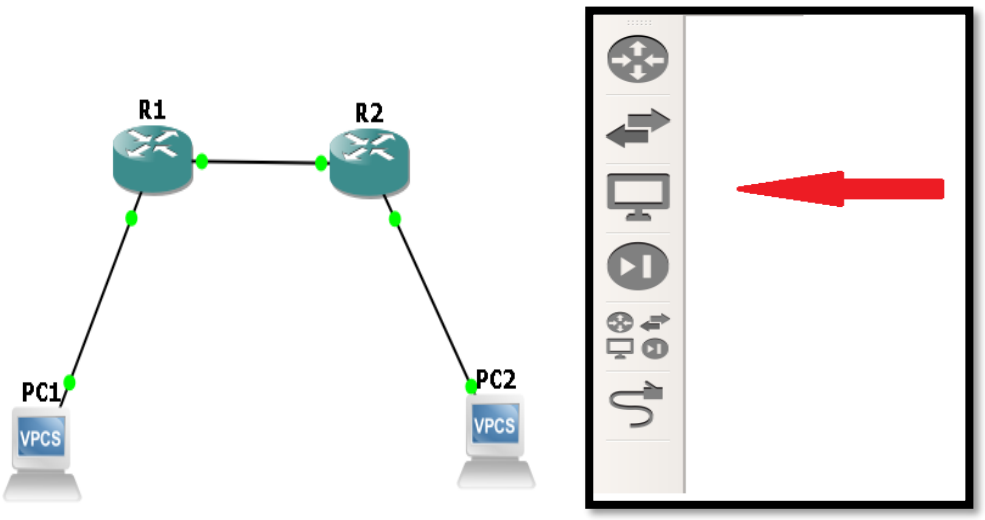


6. Assume a network with the topology as the following figure. All the links are bidirectional. The link length (in kilometers, not capacity) is labeled within each link. Using any mathematical equations or models to formulate the Shortest-Path (from s to t) problem of the network. (Hint: need specific the notations, goal, and …)



Part II: A lab on IP addressing and routing

1. Download GNS3 and install
    a. For windows, when prompted for “choose components”, uncheck “SolarWinds Response Time Viewer”.
    b. Download the Cisco IOS image “c2600-ik8o3s-mz.122-11.T.bin”.
    c. Start GNS3 and browse to select the above Cisco IOS image on your computer. Make sure use the follow setting:
        - Name: c2600
        - Platform: c2600
        - Chassis: 2611XM
        - Memory size 64Mb
        - slot 0: C2600-MB-2FE
        - slot 1: NM-1FE-TX
        - Wic 0: WIC-1T
2. Use “Local sever” to start a new GNS3 project and design the following network topology. You can use the left bar to drag and drop the network devices. After designing the topology hit the play button (green).



3. **IP address**: Configure the above network using the console for each device (you can right click on each device to get access to the console) and test the reachability between PC1 and PC2. Each interface on the devices should be configured.

Assume your Panther ID is “N9N8N7N6N5N4N3N2N1” Develop an addressing plan and make sure the first subnet address is “192.168.N1.0”; the second subnet address is “192.168.N2.0”; the third subnet address is “192.168.N3.0”,… and so on.

Question 1:

- How many subnets are there in the network? List all the subnets.
- List all the IP address and MAC address of all the interfaces in the network.

- Use the ping command to test if PC1 and PC2 can reach each other; explain the test results; and show a screenshot of this.

4. **Static Routing**: Issue "no ip routing" to clear the previous routing information. Use IOS command "ip route …." to configure both routers to make sure PC1 and PC2 can reach each other.

   Question 2:

   - List the commands on R1 and R2 to configure the static routing
   - Use the ping command to make sure PC1 and PC2 can reach each other; explain the test results; and show a screenshot of this.

5. **Dynamic Routing with RIP**: Issue "no ip routing" to clear the previous routing information. Use IOS command "router rip" to configure both routers to make sure PC1 and PC2 can reach each other.

   Question 3:

   - List the commands on R1 and R2 to configure the routing
   - Use the ping command to make sure PC1 and PC2 can reach each other; explain the test results; and show a screenshot of this.

6. **Submission**: A hard copy and a soft copy of the report are needed. The soft copy should be submitted to the course dropbox in iCollege.

Appendix: IOS commands and examples

- **An example of configuring Cisco router interfaces**

```
Router1> enable
Router1# configure terminal
Router1(config)# no ip routing
Router1(config)# ip routing
Router1(config)# interface FastEthernet0/0
Router1(config-if)# ip address 10.0.2.1 255.255.255.0
Router1(config-if)# no shutdown
Router1(config-if)# interface FastEthernet0/1
Router1(config-if)# ip address 10.0.3.1 255.255.255.0
Router1(config-if)# no shutdown
Router1(config-if)# end
```

- **An example of adding a specific route in Cisco routers**

The command bellow is to add a host route to host IP address `10.0.2.65` with the next-hop set
to `10.0.1.21`. In IOS, a host route is identified by a 32 bit prefix.

```
Router1(config)# ip route 10.0.2.65 255.255.255.255 10.0.1.21
```

- **An example of configuring RIP**

```
Router1>enable
Router1#configure terminal
Router1(config)#no ip routing
Router1(config)#ip routing
Router1(config)#router rip
Router1(config-router)#version 2
Router1(config-router)#network 10.0.0.0
Router1(config-router)#interface FastEthernet0/0
Router1(config-if)#no shutdown
Router1(config-if)#ip address 10.0.1.1 255.255.255.0
Router1(config-if)#interface FastEthernet0/1
Router1(config-if)#no shutdown
Router1(config-if)#ip address 10.0.2.1 255.255.255.0
Router1(config-if)#end
```