George Mavroeidis

COMP 445 M Theory Assignment 3

For Dr. Sandra Cespedes

1. **TCP**
   1. **Consider two TCP connections, one between Hosts A (sender) and B (receiver), and another between Hosts C (sender) and D (receiver). The RTT between A and B is half that of the RTT between C and D. Suppose that the senders’ (A’s and C’s) congestion window sizes are identical. Is their throughput (number of segments transmitted per second) the same? Explain.**

If we consider that the amount of unacknowledged data at the sender is solely limited by cwnd. We also consider that loss and packet transmission delays are negligible. Then, roughly, at the beginning of every RTT, the constraint permits the sender to cwnd bytes of data into the connection; at the end of the RTT the sender receives acknowledgments for the data. Thus, the sender’s send rate is roughly cwnd/RTT bytes/sec. In our case, The RTT between A and B is half of that of the RTT between C and D. Therefore, A’s send rate is double of that of C and their throughput is not the same.

* 1. **Now suppose that the average RTT between A and B, and C and D are identical. The RTT between A and B is constant (never varies), but the RTT between C and D varies considerably. Will the TCP timer values of the two connections differ, and if so, how are they different, and why are they different?**

When the RRT varies by a considerable margin, an estimated RTT plus some margin is calculated, since the timeout can fluctuate between transmissions and retransmissions. The margin should be large when there is a lot of fluctuation in the sample RTT values, which is a collection of previous timeouts recorded that are used to evaluate the current estimated RTT.

Since RTT between A and B is constant, the RTT is also constant (never varies. The RTT between C and D varies considerably, meaning that the TCP timer values of the two connections differ due to the mentioned reasons above.

* 1. **Give one reason why TCP uses a three-way (SYN, SYNACK, ACK) handshake rather than a two-way handshake to initiate a connection.**

There are many reasons why TCP uses a three-way handshake, but the most important ones are to establish a reliable connection and to ensure no duplicates of connection initiations occur. Without the three-way handshake, both the server and the client would not be able to establish a connection between them and acknowledge it. A two-way handshake would only allow one side to send data and both client and server would not be synchronized with their sequence numbers. TCP is a bi-directional communication protocol and a three-way handshake ensures both parties acknowledge each other’s presence and the data they are sending and receiving to one another.

1. **IP addressing.**
   1. **Write the IP address 129.17.129.97 in its binary form.**

Using the 8-but binary form, we can easily interpret the binary form for each number by representing it in powers of 2:

10000001.00010001.10000001.01100001

* 1. **Consider an IP subnet with prefix 129.17.129.97/27. Provide the range of IP addresses (of form xxx.xxx.xxx.xxx to yyy.yyy.yyy.yyy) that can be assigned to this subnet.**

Since we already calculated the binary form, the next step is to calculate the subset address using the binary notations. To do this, a bit-wise AND operation will be performed. This operation is between the binary forms of the host IP address and the subnet address. Once it is calculated, the decimal number of the subnet address will be found.

+

Network Bits

Subnet Bits

Host Bits

Since 5 bits from the Class C address are used, there are 3 bits left to define hosts within a particular subnet. Now the broadcast, first and last notes will be determining:

First Host:

Last Host:

First Subnet:

Last Subnet:

Broadcast:

The number of hosts per subnet is: 2^5 – # Broadcast – # Subnet Address

The range of IP Addresses are between The First Host and the Last Host, including the Broadcast addresses:

Decimal of First Address: 129.17.129.96

Decimal of Broadcast: 129.17.129.127

* 1. **Suppose an organization owns the block of addresses of the form 129.17.129.97/27. Suppose it wants to create four IP subnets from this block, with each block having the same number of IP addresses. What are the prefixes (of form xxx.xxx.xxx/y) for the four IP subnets?**

Since we want to divide into four subnets, we will use subnet prefix of +2 bits (since 4 in binary is 11). Therefore, we will use a subnet prefix of 27 + 2 = 29 bits. The prefix will look like 129.17.129.01100XXX/29. This leaves us with 3 bits for each block. Therefore, 127 – 96 + Broadcast + Subnet for broadcast = 32 # of hosts for the subnet. These 32 # of hosts will be split among the four IP subnets for the specified block. Therefore, each subnet will have 8 hosts, leaving us with the following ranges:

* 129.17.129.96/29 - 129.17.129.103/29
* 129.17.129.104/29 - 129.17.129.111/29
* 129.17.129.112/29 - 129.17.129.119/29
* 129.17.129.120/29 - 129.17.129.127/29

1. **IP Addressing**

**The computer I am using on my home Wi-Fi connection has the IPv4 address 10.0.0.2. I am playing a multi-player computer game which uses a P2P architecture for its network traffic between players. My friend is playing the same computer game as me and in casual conversation tells me that their computer also has the IPv4 address 10.0.0.2 on their home internet connection. Two hosts on the same network such as the internet can not share the same IP address AND communicate with each other at the same time.**

* 1. **Is there anything special about the IP range 10.0.0.0/8 and are there other ranges with a similar role?**

What it means is that there are 8 bits used for the network prefix, meaning there are 24 bits left over in the network to contain IPv4 host addresses in range 10.0.0.0 to 10.255.255.255 in decimal enumeration.

* 1. **Is there anything special about how my home router is routing network traffic?**

It means that both players are playing a multiplayer video game from the same private network and that the home has a NAT router. Since both users are behind a NAT router, it means that to connect to the WAN and communicate with each other, there is one single IP Address for both users.

* 1. **How is the issue of duplicate IP addresses handled in this case?**

To fix this, UPnP (Universal Plug N Play) or port forwarding manually can be the main solutions. UPnP allows a host to discover and configure a nearby NAT and allows the game itself to access the ports behind the router’s firewall and forward them to itself. If done manually, Hamachi can be used to manually port forward in order to accommodate users with the same IP address to communicate and play the same games.

* 1. **How is a connection opened between my computer and my friend’s computer so that we can play this game together?**

Port forwarding allows the game to identify the hosts within a network that uses a NAT router. Therefore, the connection is passed through the internet using a single IP address, but within the NAT router, ports are used to address hosts instead of processes.

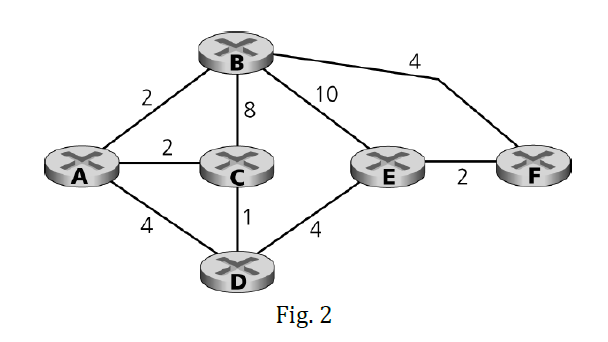
1. **Consider the network shown if Fig. 1**
   1. **Show the operation of Dijkstra’s (link-state) algorithm for computing the least cost path from D to all destinations.**
   2. **What is the shortest path from D to B? What is the cost of the path?**



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **A** | **B** | **C** | **E** | **F** |
| **Step** | **N’** | **D(A), p(A)** | **D(B), p(B)** | **D(C), p(C)** | **D(E), p(E)** | **D(F), p(F)** |
| 0 | D | 4, A | ∞ | 1, C | 4, D | ∞ |
| 1 | DC | 3, C | 9, C |  | 4, D | ∞ |
| 2 | DCA |  | 5, A |  | 4, D | ∞ |
| 3 | DCAE |  | 5, A |  |  | 6, E |
| 4 | DCAEB |  |  |  |  | 6, E |

* **D to A:** → 3, DCA
* **D to C:** → 1, DC
* **D to E:** → 4, DE
* **D to B:** → 5, DCAB (b. also shortest path from D to B, has lowest cost)
* **D to F:** → 6, DEF

1. **Consider the network in Fig. 2**
   1. **What are A, B, C, D, E, and F’s distance vectors? Note: you do not have to run the distance vector algorithm; you should be able to compute distance vectors by inspection. Recall that a node’s distance vector is the vector of the least cost paths from itself to each of the other nodes in the network.**
   2. **Now consider node C. From which other nodes does C receive distance vectors?**
   3. **Consider node C again. Through which neighbor will C route its packets destined to E? Explain how you arrived at your answer, given the distance vectors that C has received from its neighbors.**

****

**A.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Node** | **A** | **B** | **C** | **D** | **E** | **F** |
| **A** | 0 | 2 | 2 | 3 | 7 | 6 |
| **B** | 2 | 0 | 4 | 5 | 6 | 4 |
| **C** | 2 | 4 | 0 | 1 | 5 | 7 |
| **D** | 3 | 5 | 1 | 0 | 4 | 6 |
| **E** | 7 | 6 | 5 | 4 | 0 | 2 |
| **F** | 6 | 4 | 7 | 6 | 2 | 0 |

**B.**

Receives distance vectors from A, B and D, but not from nodes E and F (only direct neighbours)

**C.**

To find minimum cost path, find all possible paths from C and its neighbours that go to E with the cost formula of the cost between C and its neighbor plus distance vector from neighbor to next neighbor until goal. In this case, the distance vector is between C’s neighbors and the goal node E directly.

* c(C,B) + DB(E) = 8 + 6 = 14
* c(C,A) + DA(E) = 2 + 7 = 9
* c(C,D) + DD(E) = 1 + 4 = 5

1. **Consider the network in Fig. 3 in which network Wis a customer of ISP A, network Y is a customer of ISP B, and network X is a customer of both ISPs A and C.**
   1. **What BGP routes will A advertise to X?**

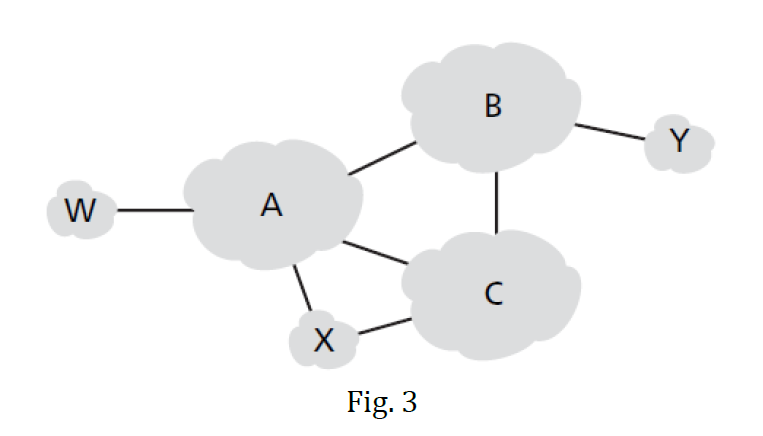
A advertises to X route AW, but won’t advertise AW to C, because it does not get any revenue from it and gives C a free route. A will also advertise route ABY to X, but not to C for the same reasons above.

* 1. **What routes will X advertise to A?**

X won’t advertise any route from A to C, so X won’t advertise anything.

* 1. **What routes will A advertise to C? For each answer provide a one-sentence explanation.**

A will not advertise route ABY or AW to C, but will force C to take route B for reaching Y. It won’t advertise any source/destination routes of its customers to other ISP’s.

****

1. **Describe the main role of the communication layer, the network-wide state-management layer, and the network-control application layer in an SDN controller.**

The communication layer is a protocol layer that constitutes the lowest layer of the controller architecture and provides communication between the SDN controller and the controlled network devices via the controller’s “southbound” interface. It transfers information between the controller and those devices as well as the device’s events that are locally observed. These events must be communicated with the controller. All these information are provided to the network’s plane OpenFlow is a specific protocol that provides such functionalities and is implemented in most SDN controllers.

The network-wide state-management layer stores and controls decisions and information for various controlled devices. Examples of information for the controller are configuring flow tables, end-to-end forwarding and firewalling capabilities. The controller must have all these information copied and up to date, mostly about the state of the networks’ hosts, links, switches and other SDN-controlled services. The SDN controller is in the middle of the API and stores all the information mentioned above.

The network-control application layer is the interface that interacts with network-control applications. It is utilizing the Northbound API to read/write network state and flow tables of network-control applications within the state-management layer. Basically, it passes all the information to the controller in order to process them and make important automated decisions for their requirements in the most optimal way. REST is a request-response interface that is used by many SDN controllers to communicate with their applications.

1. **Compare the match-plus-action operation in a traditional network versus an SDN-based network**
   1. **What would be the operation (mapping and action taken) when using destination-based forwarding in a traditional network?**

The match-plus-action operation in a traditional network occurs when a packet arrives at a router or a switch and is ready to be forwarded based on the packet’s information, most importantly the destination address. The destination addresses and the path interface to reach that destination are the two fields within the destination address.

Firstly, the destination address is compared with the forwarding table and attempts to find a match to execute the corresponding action. If the match is found, forwarding takes place, which means the packet is ready to be encapsulated and proceed to the next destination route. If no match is found, no action will take place, which means the packet will be dropped or discarded.

* 1. **Mention two fields that could be matched in a match-plus-action rule applied in an SND-based network. Also mention the possible actions to be applied to a packet that conforms a matching rule.**

Two fields that could be matched in a match-plus-action rule in an SDN-based network are source and destination IP Addresses. Possible actions to be applied to a packet that confirms a matching rule are: forwarding, modifying fields and packet dropping.