EE4204 Homework 3 Zhuang Jianning
A0214561M

1. What are the benefits of IPv6 over IPv4?

The main difference between IPv4 and IPv6 is the address size of the IP addresses. IPv4 is a 32-bit address which can support 2^32 or around 4 billion IP addresses. However, these 4 billion addresses are already almost all being utilized, hence a need for a larger address space. IPv6 which is a 128-bit address resolves this issue and will be sustainable for a long time.

IPv6 also specifies a new packet format and a simpler packet header, designed to minimize packet header processing by routers. Many rarely used fields are also moved to optional header extensions.

Other benefits of IPv6 over IPv4 include no more NAT (Network Address Translation), auto-configuration, no more private address collisions, better multicast routing, simpler header format, simplified and more efficient routing, true quality of service (QoS), also called "flow labeling", built-in authentication and privacy support, flexible options and extensions and easier administration (no more DHCP).

2. Describe both Link-State & Distance Vector approaches to routing.

<u>Link State Routing</u>

In link-state routing, each router attempts to construct its own internal map of the network topology. At the initial stage of start-up, when a router becomes active, it sends the messages into the network and collects the information from the routers to which it is directly connected. It also provides information about whether the link to reach the router is active or not. This information is used by other routers to build a map of network topology. Then the router uses the map to choose the best path.

The link state routing protocols respond swiftly to the network changes. It sends triggered updates when a network change occurs and sends periodic updates at long time intervals such as 30 minutes. If the link alters state, the device detected the alteration generates and propagates an update message regarding that link to all routers. Then each router takes a copy of the update message and updates its routing table and forwards the message to all neighboring routers.

This flooding of the update message is needed to ensure that all routers update their database before creating an update routing table that reflects the new technology. OSPF protocol is the example link state routing.

Distance Vector Routing

In distance vector routing, a router need not know the entire path to every network segment; it only requires to know the direction in which to send the packet. The technique determines the direction (vector) and distance (hop count) to any network in the internetwork.

Distance vector routing algorithms periodically send all or parts of their routing table to their adjacent neighbors. The routers running a distance vector routing protocol will automatically send periodic updates even if there are no changes in the network.

A router can verify all the known routes and alter its local routing table on the basis of the updated information received from neighboring routing. This process is referred to as “routing by rumor” because the routing information that a router has of the network topology is based on the perspective of the routing table of the neighbor router.

RIP and IGRP is a commonly used distance vector protocol that uses hop counts or its routing metrics.

Differences between Link State and Distance Vector Routing

Bellman-Ford algorithm is used for performing distance vector routing whereas Dijkstra is used for performing the link state routing.

In distance vector routing the routers receive the topological information from the neighbor point of view. In link state routing the router receives complete information on the network topology.

Distance vector routing calculates the best route based on the distance (fewest number of hops) while link state routing calculates the best route on the basis of least cost.

Link state routing updates only the link state while Distance vector routing updates the full routing table.

The frequency of update in both routing techniques is different distance vector update periodically whereas link state update frequency employs triggered updates.

The distance vector routing is simple to implement and manage. In contrast, the link state routing is complex and requires trained network administrator.

The convergence time in distance vector routing is slow, and it usually suffers from count to infinity problem. Conversely, the convergence time in link state routing is fast, and it is more reliable.

3. Classify RIP/OSPF/BGP according to the following metrics: LS or DV, Intra-AS or Inter-AS, Centralized or Distributed.

Routing Information Protocol (RIP) => Distance Vector, Intra-AS and Distributed

Open Shortest Path First (OSPF) => Link State, Intra-AS and Centralized

Border Gateway Protocol (BGP) => Distance Vector, Inter-AS and Distributed

4. Many network engineering problems are about resource allocation – namely the allocation of a set of finite resources amongst users with certain needs. Suppose there are 3 users competing for a 90 mbps link. Users 1 and 2 want 50 mbps each and User 3 wants 10 mbps. My solution is to give each one 30 mbps. Is this fair?

It depends on the definition of fairness in that context.

Giving each user 30Mbps is an equal distribution of bandwidth which could be considered fair.

There is also proportional fairness where each user gets bandwidth proportional to what they requested/need. In this case, total demand is 110Mbps on a 90Mbps link. User 1 and 2 would get 50*90/110 = 40.9Mbps each while User 3 will get 10*90/110 = 8.2Mbps

There is also Max-Min fairness which aims to maximize the minimum resource of any flow. This means that small flows receive what they demand and larger flows share the remaining capacity equally. In this case, User 3 will get 10Mbps while User 1 and 2 share the remaining 80Mbps by getting 40Mbps each.

5. We discussed max-min fairness in class. What is the max-min fair allocation? What is the TCP fair solution?

Max-min fairness is said to be achieved by an allocation if and only if the allocation is feasible and an attempt to increase the allocation of any flow necessarily results in the decrease in the allocation of some other flow with an equal or smaller allocation. A max-min fair allocation is achieved when bandwidth is allocated equally and in infinitesimal increments to all flows until one is satisfied, then amongst the remainder of the flows and so on until all flows are satisfied or the bandwidth is exhausted. In the case of the previous example, User 3 will get 10Mbps while User 1 and 2 share the remaining 80Mbps by getting 40Mbps each.

TCP fairness requires that a new protocol receive a no larger share of the network than a comparable TCP flow. This is important as TCP is the dominant transport protocol on the Internet, and if new protocols acquire unfair capacity they tend to cause problems such as congestion collapse.

6. Consider the communication graph below. The edge labels are of the form a / b, where a is the cost in dollars of using that link and b is the delay in seconds of using that link. Run Dijkstra's algorithm on this graph and find the optimal route from A to E.

Optimal Cost

V	D(B)/p(B)	D(C)/p(C)	D(D)/p(D)	D(E)/p(E)
A	2/A	3/A	3/A	inf
AB		3/A	3/A	8/B
ABC			3/A	8/B
ABCD				7/D
ABCDE				

V	D(B)/p(B)	D(C)/p(C)	D(D)/p(D)	D(E)/p(E)
A	2/A	3/A	3/A	inf
AB		3/A	3/A	8/B
ABD		3/A		7/D
ABDC				7/D
ABDCE				

In both cases of the tiebreaker between nodes C and D, the optimal cost route from A to E is through A-D-E by following the predecessor pointer from node E

Optimal Delay

V	D(B)/p(B)	D(C)/p(C)	D(D)/p(D)	D(E)/p(E)
A	6/A	1/A	4/A	inf
AC	5/C		4/A	inf
ACD	5/C			8/D
ACDB				7/B
ACDBE				

The optimal delay route from A to E is through A-C-B-E by following the predecessor pointer from node E

7. For the communication graph above, state the distance vector table that would be computed by node D using the distance vector algorithm.

Optimal cost table at node D

Src\Dest	D(A)	D(B)	D(C)	D(D)	D(E)
A	0	2	3	3	7
C	3	2	0	2	6
D	3	4	2	0	4
E	7	6	6	4	0

Optimal delay table at node D

Src\Dest	D(A)	D(B)	D(C)	D(D)	D(E)
A	0	5	1	4	7
C	1	4	0	3	6
D	4	6	3	0	4
E	7	2	6	4	0

Node D maintains distance vector to all nodes as well as neighbors (A, C and E)

8. Did you notice that the previous two questions (6 &7) were not well defined? Remember that when you see the word “optimal”, you should first ask what is the optimality metric? Is it cost Or is it delay? Compute both the delay optimal route and the cost optimal routes.

Optimal Cost

V	D(B)/p(B)	D(C)/p(C)	D(D)/p(D)	D(E)/p(E)
A	2/A	3/A	3/A	inf
AB		3/A	3/A	8/B
ABC			3/A	8/B
ABCD				7/D
ABCDE				

V	D(B)/p(B)	D(C)/p(C)	D(D)/p(D)	D(E)/p(E)
A	2/A	3/A	3/A	inf
AB		3/A	3/A	8/B
ABD		3/A		7/D
ABDC				7/D
ABDCE				

In both cases of the tiebreaker between nodes C and D, the optimal cost route from A to E is through A-D-E by following the predecessor pointer from node E

Optimal Delay

V	D(B)/p(B)	D(C)/p(C)	D(D)/p(D)	D(E)/p(E)
A	6/A	1/A	4/A	inf
AC	5/C		4/A	inf
ACD	5/C			8/D
ACDB				7/B
ACDBE				

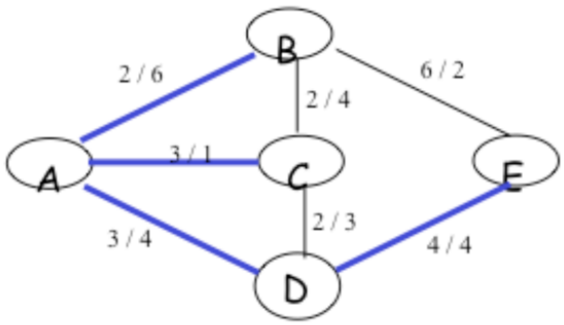
The optimal delay route from A to E is through A-C-B-E by following the predecessor pointer from node E

9. In the resource allocation problem, you were asked to compute a “fair” solution. Again, you need to ask first what is the fairness metric? What are some notions of fairness?

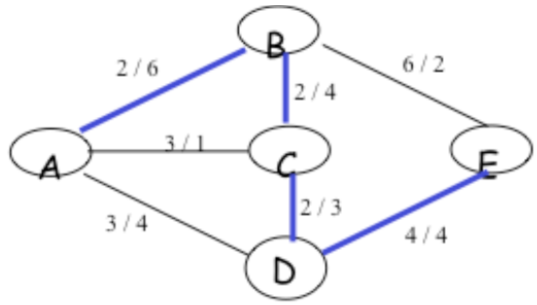
Equal Distribution Fairness
Proportional Fairness
Max-min Fairness
Jain's Fairness Index
QoE Fairness

10. Compare the Dijkstra Shortest Spanning Tree to the Minimum-cost Broadcast Spanning Tree for the graph in Question 6.

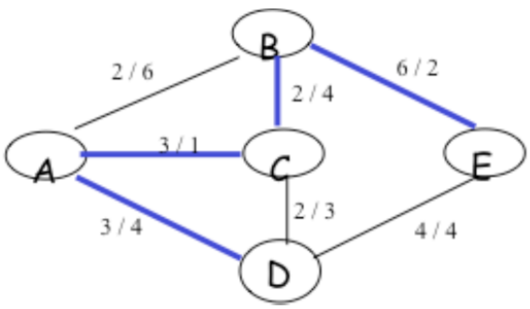
Dijkstra from A (cost)



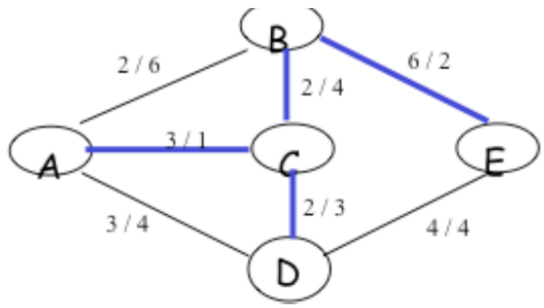
Broadcast from A (cost)



Dijkstra from A (delay)



Broadcast from A (delay)



Broadcast done using prim/kruskal

11. Consider a wireless network. Does carrier sensing always work in wireless networks? What MAC does WiFi (802.11) use? Describe it and compare it to the MAC used in Ethernet.

Carrier Sensing does not always work in a wireless network due to the hidden node problem where 2 nodes who are unaware of each other send signals to a common node reachable by both, resulting in a collision.

WiFi (802.11) uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
While Ethernet uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

This is because WiFi might not be able to detect all collisions due to hidden node and exposed node problem and uses RTS and CTS to avoid collisions.