Assignment 6

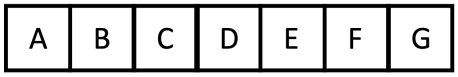
CS 181AG: Network Algorithmics

Due: Oct 11, 2022 10pm PT

In this assignment,you will explore how to make a binary search more efficient and gain practice with packet classification by creating a small firewall. The assignment also includes a reading and writing component.

Problem 1: Improving Binary Search. In class, we learned about how binary search can be used on prefix lengths to perform IP lookup. In this problem, we'll look at how to improve the throughput of binary search. For simplicity, we'll consider the problem of looking for elements in an array, but the results can be extrapolated to prefix lengths.

Suppose we have 7 elements total, arranged in 7 contiguous memory locations as shown below. Binary search is performed using a pointer to keep track of which element we are comparing against. While a single search takes O(log n), we wonder whether we can have multiple ongoing searches at once. However, we quickly run into a problem if multiple searches need to probe the same location in memory.



Without using extra memory, explain how we can increase the throughput of binary search lookups while avoiding the problem of multiple probes to the same memory location. What is the maximum number of searches that can be in progress simultaneously in this example?

Answer 1:

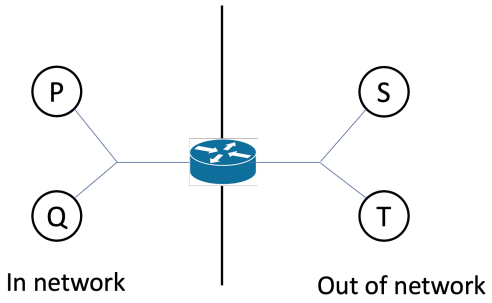
One way that we can increase the throughput of binary search lookups while avoiding the problems of multiple probes to the same memory location is by allowing the binary searches for different elements to overlap with one another. We can do this by enqueuing different searches and then ensuring that we do not allow any searches to access the same element by allowing each successive search to begin after the previous search has decided which element to access next. For example, we would allow one search to begin at the element "D", and then once the search decided to restrict itself to the left or right half of the array and accesses the next element in its search (or is completed), then we would allow the next search to access "D", and so forth. For example if we were searching for elements, "A", "B", "F", then we would allow our first search to access "D", then once it realizes that it will focus on the left half of the array, then it will access "B", and at the same time the search for "A" will begin by accessing "D". Finally, the first search would then access "A", the second accessing "B", and the final search would begin at "D".

Problem 2: Building a Firewall. In this problem, you will construct the rules for a small firewall and build two types of tries from your rule database.

1. Let's first build the rule database for the router pictured below. It sits at the edge of a network. Two devices, P and Q, are connected to the network. S and T are two devices outside the network. The relevant IP prefixes/addresses are provided here. For simplicity, assume IPs are only 4 bits long instead of 32.

   Network prefix: 01*; P: 0101; Q: 0110; S: 1010; T: 1101

   Our firewall applies different rules based on the contents of the packet headers. The following table lists the criteria to identify the packet function.



mail: Dst. port = 25

file transfer: Dst. port = 20

TCP acknowledgements: TCP_ack flag is set

remote login request: Dst. port = 22

Fill in the table below based on the following rules. The rules are in order of least to greatest cost.

Apply Rule **R1** when S sends mail to P

Apply Rule **R2** when T transfers files to any device in the network

Apply Rule **R3** when S sends a remote login request to any device in the network

Apply Rule **R4** for any traffic originating from the network

Apply Rule **R5** when any device sends a TCP acknowledgement to any device in the network

Apply Rule **R6** for any traffic at all

Rule	Dst IP	Src IP	Dst Port	Src Port	Flags
R1	D1 = 0101	S1 = 1010	25	-	-
R2	D2 = 01*	S2 = 1101	20	-	-
R3	D3 = 01*	S3 = 1010	22	-	-
R4	D4 = *	S4 = 01*	*	-	-
R5	D5 = 01*	S5 = *	*	-	TCP ack
R6	D6 = *	S6 = *	*	*	*

2. Similar to in class, let's solve a simpler problem by only focusing on classifying packets based on the source and destination IP addresses. In other words, take the table you filled in above, and for this sub-problem, only consider the columns for Rule, Dst IP, and Src IP.

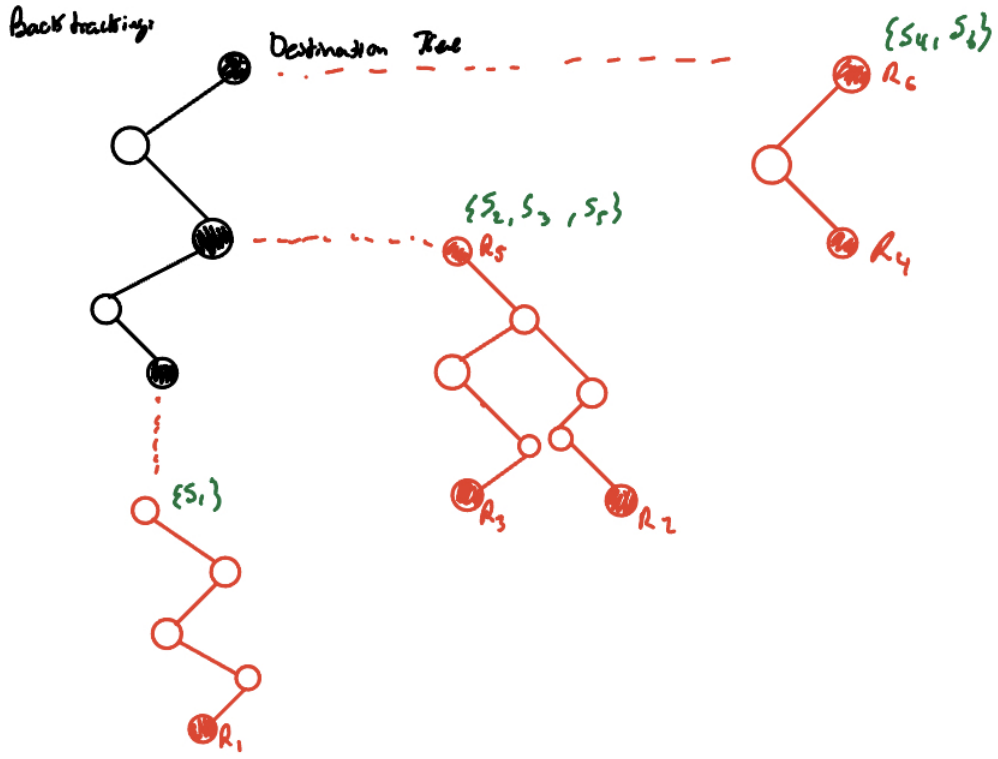
   Your task here is to draw two versions of the trie of tries.

   (a) The first version is the one you would use with the backtracking algorithm. Similar to class, we start with the destination trie at the top, and each valid prefix points to a source trie. In this version, each of {S1, S2, ..., S6} is present in exactly one source trie.

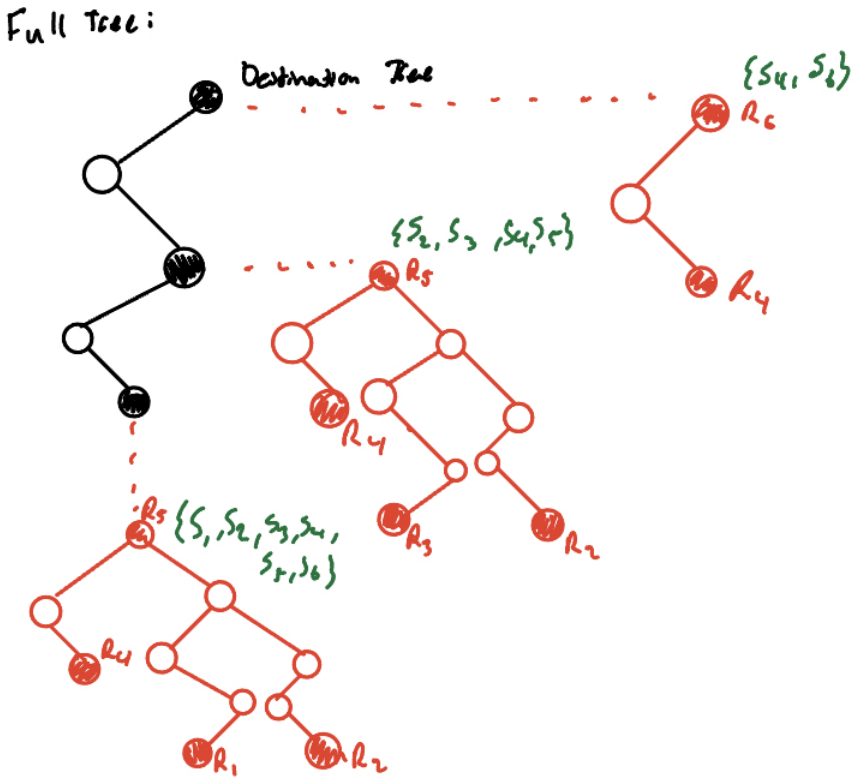
   (b) In the second version, once the algorithm follows a pointer to a source trie, it does not leave that trie, so each trie must contain all necessary entries from {S1, S2, ..., S6}. Similar to class, we start with the destination trie at the top, and each valid prefix points to a source trie.

   Notes: In both drawings, please distinguish clearly between destination and source tries, i.e., different color or dashed lines between them. Please also label which nodes in the source trie correspond to rules by labelling them, i.e., R1, R2, etc. If a node matches multiple rules, only label it with the best rule. Finally, remember to add arrows such that **every** destination trie node points to the source trie corresponding to its best matching prefix.

Answer 2:



Full Tree:



Problem 3: Reading. We looked at firewalls in Problem 2, but another reason to look at multiple fields in a packet header is treat certain traffic differently with regards to quality of service. Your reading assignment this week is to research the problem of network neutrality. Then, write an explanation to a friend (2-3 paragraphs) who understands basic networking terms but does not know what net neutrality is, explaining the following 1) How does network discrimination work? 2) What are the main arguments for and against net neutrality?

I found this article to be helpful in presenting the technical details, but you may use any source you'd like (please cite the sources you used).

Answer 3:

Network discrimination can occur in a couple of different ways as described by the author. The discrimination arises from the situation where congestion on an internet network causes the routers to drop particular packets in order to relieve congestion. The first type of discrimination described by the author is called "minimal discrimination", which occurs in this situation when the router needs to drop packets to alleviate the traffic. In this instance, the network alleviates the traffic by discarding lower-priority packets when necesssary. In all other instances for minimal discrimination, the low priority packets do not play second fiddle to the high-priority packets. However, in "non-minimal" discrimination, routers can limit the network capacity that low-priority packets can access, which can lead to the discarding of low-priority packets before the network is at its capacity. While the first may assist the speed of high-priority packets to being delivered, especially in moments when the network is congested, the second does not help out high-priority packets, but simply serves to disservice the low-priority packets. There can also be delay discrimination which can occur during buffering, in which minimal discrimination will give buffering priority to the high-priority packets and the non-minimal discrimination would result in the slowing of low-priority packets even when there is network capacity to send the packet.

The main arguments against network neutrality is that ISPs have the ability to currently discriminate different types of traffic based on priority which can lead to future manipulations of peoples network speeds which can inturn force individuals to pay more of internet service to prevent the kind of discrimination described above. Similarly, ISPs can impose discrimination on different types of traffice that a user produces, which can in turn force users away from using different applications if the ISPs can determine from where the traffic comes from and it happens to be a product that they want to disincentive users from. The argument is that these freedoms and capabilities give ISPs far too much power that they can leverage to hurt consumers financially and with respect to their choices of products to use on networks. However, some argumetns against net neutrality are that Quality of Service gaurentees for different types of traffic such as video are supported by network providers. However, with the imposing of net neutrality rules, by forcing all types of traffic to be treated the same by routers would have the unintended conflict of negatively affecting traffic such as video by not allowing for QoS gaurentees for said forms of browsing and internet access. Similarly, arguments against net neutrality argue that enforcing net neutrality rules would be error prone as well as difficult to even do.

Problem 4. How long did this assignment take you?

Answer 4:

This assignment took me ≈ 6 hours.