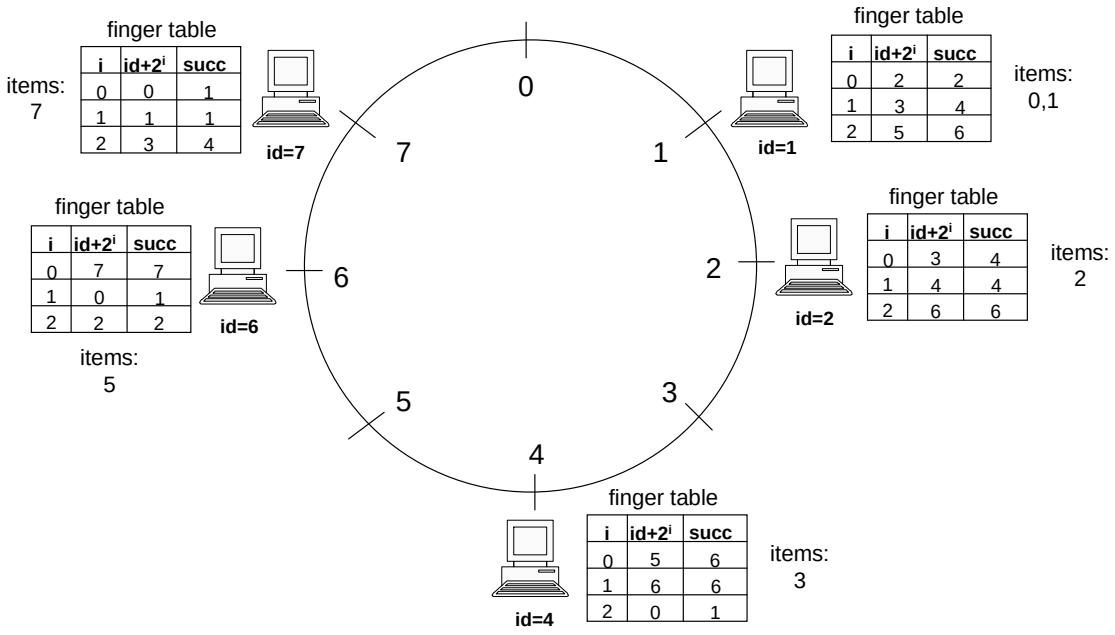
15-441: Computer Networks
Optional Homework 4

Assigned: Nov 20, 2007
Due: Nov 29, 2007

1 DHTs

1. Albert, in fear that the RIAA will shut down his centralized P2P server (like Napster), sets up a Chord DHT for lookups and routing in his peer to peer network. Unfortunately (or fortunately, for you), Dave's P2P network is not very popular and only consists of five peers at the moment with finger tables and items illustrated below. For example, *node 4* has *item 3*.

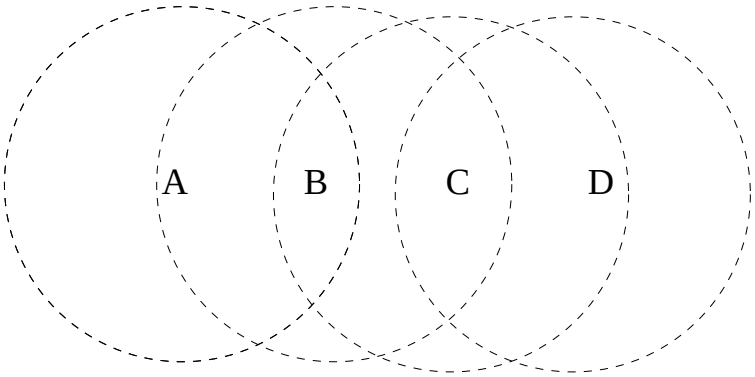


(a) List the nodes that will receive a query from *node 2* for *item 0*.

(b) Suppose node 4 crashes. *node 7* queries for *item 5*. List the nodes that will receive this query, assuming the the tables have had time to converge after noticing that node 4 has left.

2 Wireless

2. Consider the following topology of wireless laptops A, B, C and D. The dotted lines indicate the range of wireless transmissions from each node. For example, B is within range of A, A & C are within range of B, B & D are within range of C and only C is within range of D.



Assume that each node uses an RTS/CTS based MAC protocol (i.e. like MACAW)

(a) If C is sending B an RTS, why does A know not to transmit?

(b) If B is sending data to C, why does D know not to transmit?

(c) Using the nodes above, give an example of the hidden terminal problem.

(d) Irene Packet is considering implementing a walkie-talkie service for her wireless PDAs. Her program largely uses small packets to avoid delaying any voice. Should Irene use RTS/CTS for her deployment? Why?

3 Quality of Service

3. Consider 10 flows with arrival rates of 1,2,...,10 Mbps that traverse a link of 50Mbps. Calculate the max-min fair share on this link. What is the fair share if the link capacity is 60 Mbps?

4. Suppose a router has accepted flows with the token bucket parameters shown in Table 1. All flows are in the same direction, and the router can forward one packet every 0.1 seconds.

Token Rate	Bucket Size
1	10
2	4
4	1

Table 1: Token bucket parameters

(a) What is the maximum delay a packet might face?

(b) What is the minimum number of packets from the third flow that the router would send over 2 seconds, assuming that the flow sent packets at its maximum rate of 4 packets/second uniformly?

4 Security

5. Scenario: U.S. and Russia signed a comprehensive nuclear test-ban treaty. To verify the compliance of the treaty, seismic monitoring systems must be installed to detect any underground testing of nuclear weapons, Such monitoring systems are physically secure (tamper-proof) and are installed in the host nation near certain test sites. The data they collect is transmitted back to the monitoring nation (the host nation can also listen to the transmission), and this data will include timestamps to prevent any replay attacks. Let's assume in this problem the host nation is Russia, and the monitoring nation is the U.S.

   Requirements

   - The U.S. needs to ensure that the data it receives from the monitoring system is not altered/forged.
   - Russia wants to verify in real time that only the seismic data (agreed on in the treaty) is transmitted, i.e. the U.S. is not sending any additional information using the communication channel.
   - If the U.S. finds evidence (from the seismic data) that Russia violates the treaty, it wants to convince the United Nations that such a violation occurred.

   The following verification systems are developed to address the above requirements. (Assume that algorithms required for these approaches exist). We ask you to identify the problems with each of the four approaches. Note that there may be more than one problem with each approach. In this case, if you can identify one "important" problem with an approach, you will get full credit for that approach. If, however, you only identify several "less important" problems, you may not get the full credit. *Hint: Logical flaws in algorithms/protocols are "important", while other problems are "less important". Of course, if there are no logical flaws, other problems become "important".*

   (a) The U.S. installs a secret key along with the monitoring system. When transmitting data back to the U.S., the monitoring system encrypts the transmission using a symmetric cryptographic algorithm and the secret key. How does this approach address the requirements? What are the problems with this approach (if any)?

   (b) The U.S. generates a public/private key pair and installs the private key along with the monitoring system. The public key is made available to everyone. When transmitting data back to the U.S., the monitoring system encrypts the transmission with the private key using public-key cryptography (e.g. the RSA algorithm). How does this approach address the requirements? What are the problems with this approach (if any)?

   (c) The U.S. and Russia each install a subkey along with the monitoring system (but they don't know each other's subkey). The monitoring system then constructs a private key from the two subkeys and also constructs the public key. The public key is made available to everyone, and public-key cryptography is used as in (b). How does this approach address the requirements? What are the

problems with this approach (if any)?

(d) The monitoring system automatically generates a public/private key pair. The public key is made available to everyone, and public-key cryptography is used as in (b). How does this approach address the requirements? What are the problems with this approach (if any)?

6. Sparky McFirewall has networks 10.0.2/24, 10.0.4/24 and notices that hosts 10.0.0.32, 10.0.0.252, 10.0.1.54, 10.0.3.2 and 10.0.3.129 are attacking her host 10.0.2.23. He sees that his firewall already contains:

```
deny ip to/from 10.0.0.0/25 to any
```

(a) Which hosts does this rule match?

(b) Which of the following rules would work to block the remaining hosts? (Select only one).

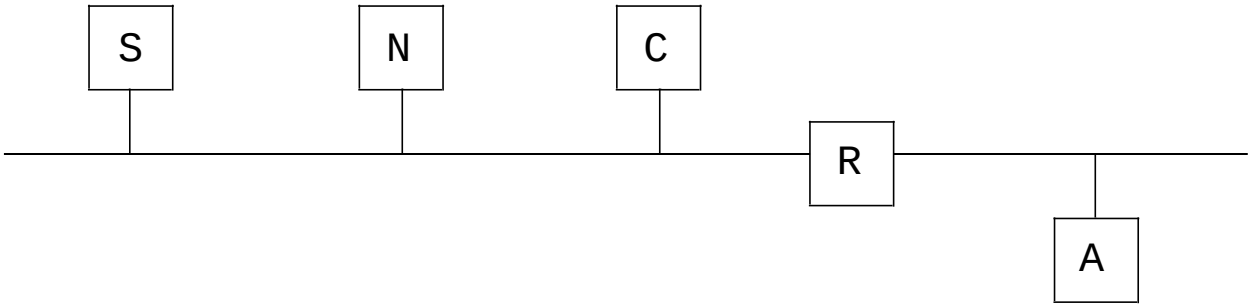
A. deny ip to/from 10.0.0.0/22
B. deny ip to/from 10.0.3.0/24
C. deny ip to/from 10.0.3.2/32, deny ip to/from 10.0.3.129/32
D. deny ip to/from 10.0.0.0/22, deny ip to/from 10.0.3.0/24,
E. deny ip to/from 10.0.0.0/23, deny ip to/from 10.0.3.0/24
F. deny ip to/from 10.0.0.0/24, deny ip to/from 10.0.1.0/23
G. deny ip from brain to paper

(c) After adding in this rule, someone complains that they can't get to a popular web site in the firewalled range. Sparky decides to allow internal users to browse Web sites in the firewalled range. Which rules need to be added? (You may not need all of the spaces below).

(d) A disgruntled employee tells the attacker about your new firewall rules. How could the attacker take advantage of these rules to continue attacking your hosts?

5 Web Transfer

In the topology shown below, machine A is a desktop client, N is a name server (but not the authoritative name server for S), C is a Web cache, R is a router and S is a Web server. Client A is configured to use Web cache C for all requests (assume that the Web cache resolves the name for any Web server and that the client is configured with the IP address of the cache). All wires/links are ethernet segments.



Assume the following:

- All the machines were just booted and their associated caches (ARP, DNS, Web, persistent connection) are all empty
- http://S/index.html fits in a single packet
- Persistent HTTP connections are used among A, C, and S (i.e. you should assume that once any connection between these hosts is established it is never closed)
- Web caches respond to TCP requests that look like packet two in table 1 below (e.g., GET http://foo/bar/). They reply with the normal web cache contents.

7. The user on machine A, requests the web page http://S/index.html. The table below shows a number of messages sent/received in servicing this request (this is not necessarily a complete list of all packets). In addition, there are a few bogus packets that are never sent/received. The packets are not listed in temporal order - fill in the order column to indicate the order in which each packet was sent/received (1=first, 2=second, etc.). Place an X in the order column if the packet is bogus.

   Table 1: HTTP Request

ID	Src	Dst	Src Port	Dst Port	Protocol	Contents	Order
1	C	DNS root		DNS	UDP	query for S	
2	A	C		Web Cache	TCP	GET http://S/index.html	
3	N	DNS root		DNS	UDP	query for S	
4	C	S		HTTP	TCP	SYN	
5	C	S		HTTP	TCP	GET index.html	
6	S	A	HTTP		TCP	index.html	
7	A	broadcast			ARP	who is R	
8	C	A	Web Cache		TCP	index.html	
9	N	C	DNS		UDP	address for S	
10	S	C	HTTP		TCP	index.html	

8. Assume that the client A has no local Web or DNS cache and that cache C has no DNS cache. However, **all** other cacheable things are cached. On a subsequent request for http://S/ index.html which of the messages from Table 1 would be eliminated (use the ID column to name the messages)?