CSC / ECE 573 Internet Protocols, Fall 2005

Homework #6

Home Syllabus Calendar Homework Project Message Board Exams Links

Due Date

- Due Tuesday, November 22, at 11:45pm

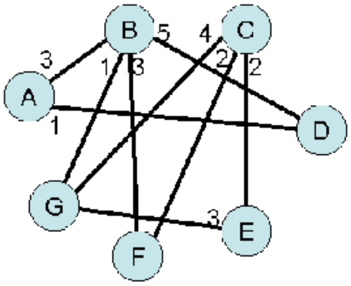
Instructions

- Homeworks should be submitted individually. We use the standard submit utility for our class to submit all work, which means your work must be prepared electronically.
- Put your name, the assignment number, and date at the top of the first page. Put solutions in order (don't make the TA hunt for your solution).
- Do not plagiarize; that means, do not copy content from any source without permission from the instructor, and if permitted, acknowledge the source.
- This homework is worth a total of 135 points

Problems

Multicast

1. Why is reliable multicast (i.e., running the equivalent of TCP for data being sent simultaneously to a group of receivers) difficult to accomplish?
2. For the following network, show the reverse path forwarding tree from a source host attached to router A to hosts reachable from routers C, E, and G.



3. IGMP does not include a strategy for acknowledgment or retransmission, even when used on networks that use best-effort delivery. What can happen if a query is lost? If a response is lost?
4. If a router has 20 entries in its group table, should it send 20 different IGMPv3 queries periodically, or just one?
5. If a router sends an IGMPv3 general query and only receives 3 reports about multicast groups, and the router is storing 5 addresses in its multicast group table, what should it do? Should it send any additional message(s)?
6. A host with IP address 142.15.13.1 and physical ethernet address 4A224512E1E2 sends an IGMPv3 membership report message about GroupID 228.45.23.11. Show all of the entries in the message.
7. Map the following IP multicast addresses to Ethernet multicast addresses. How many of them map to the same ethernet address?
    1. 224.18.72.8
    2. 235.18.72.8
    3. 237.18.6.88
    4. 224.88.12.8

BOOTP, DHCP

1. If a DHCP request is relayed, is the reply from the server sent to the relay, or to the requesting host?
2. What happens if a BOOTP client doesn't get a response to a request it sends?
3. Which of Client IP Address, Your IP Address, Server IP Address, Gateway IP Address, Client Hardware Address, and Server Name are filled in by the DHCP client, and which are filled in by the DHCP server?
4. Should a DHCP server ever set a renewal timer interval without setting the rebinding timer interval? Why or why not?
5. Can DHCP ensure that a client is not "spoofing" (i.e., can DHCP guarantee that it will never send configuration information for host A to host B)? If so, how?
6. Can a computer that uses DHCP to obtain an IP address operate as a server (i.e., can it be reached at a public address by clients on other networks)? If so, how does a client reach the server?
7. Is there a way for DHCP server to “take away” or revoke an IP address from a host before its lease period has expired? If so, what is it?

DNS

1. If you want to find out the domain name associated with the host with address 152.14.62.65, what request will you make to the DNS server (be specific)?
2. What do the Minimum and Expire fields of the SOA record control?
3. Is information in a DNS cache ever authoritative? When is information in a DNS cache purged?
4. In the following 5-node tree, how many possible zones are there? How many possible domains are there?

```
     com
    /   \
       /      \
     xyz     abc
              /  \
             /    \
          mktg   eng
```

5. Which of the following are syntatically legal domain names?
    1. com
    2. .com
    3. xyz.
    4. xyz.com.
    5. com.xyz.edu
    6. paul@xyz.edu
    7. xyz^^!-.com
    8. aaaaaaaaaaaaaaaaabbbbbbbbbbbbbbbbbbbbbccccccccccccccccccccccdddddddddddddddddddeeeeeeeeeeeeeeee.com
6. Many business computers have 3 distinct and worldwide unique identifiers. What are they?
7. A DNS client is looking for the IP address of the computer with domain name green.blue.red.com. Show the query message. Then show the response message sent by the DNS server if the IP address is found in a cache and is equal to 10.5.9.2.
8. With DNSSEC, is every resource record individually signed to authenticate its contents? Explain.
9. Use nslookup to lookup the IP address of some unusual domain name that is not likely to be locally cached (I like to use domain names of universities in remote countries for this purpose). Set nslookup to do an iterative query. Capture the resulting DNS packets using ethereal, and summarize their contents.

NAT, VPNs, Tunneling

1. Does it ever make sense to do application-layer tunneling (i.e., one application payload encapsulated inside another application payload)? If so, give an example, and if not, explain why not.
2. Does manual configuration of NAT on a "semi-permanent" basis help with address space conservation? If not, what is the value of manually configured NAT? If so, explain how it helps.
3. Suppose an organization uses VPNs to securely connect its sites over the Internet. Is there any need for a user, Jim, in this organization to use encryption or any other security mechanism to communicate with another user Mary in the same organization?
4. Consider an ICMP host unreachable message sent through two NAT boxes that interconnect three address domains, as shown below. How many address translations will occur? How many translations of protocol port numbers will occur?

```
D1 ---- NB1 ------ D2 ------ NB2 ---- D3
```

5. If NAPT rather than NAT is being used, answer the same question as above.

IPSec

1. What is the purpose of the MD5 protocol? Of the HMAC-MD5-96 protocol?
2. Can IPsec using AH be used in transport mode if one of the endpoints is behind a NAT box? Explain your answer.
3. What mandatory encryption algorithms *must* be supported by an IPSec implementation?
4. What is the overhead (additional number of bytes / packet) for ESP Tunnel Mode vs. sending a packet unencrypted? For ESP Transport mode?
5. In Kerberos authentication, what function does K_TGS(A,K_S)) in message 2 serve?
6. SUppose Cipher Block Chaining is used for a block size of 4 bits, with an initialization vector of 0011, and an encryption method which simply left circular shifts by 1 position the incoming block, and complements (flips) the leftmost 2 bits of the result (not a very strong cipher!). Show the output for the 3 successive blocks 0010 - 1100 - 1001.
7. *Extra credit* User A shares a secret key Sa with server V, and user B shares a secret key Sb with server V. User A and B wish to negotiate a shared secret key over a public communication channel such that no one, including V, will know what that secret key is. Show how they can accomplish this with the assistance of V.

Created on November 15 , 2005
Last Modified November 15, 2005
Maintained by Douglas S. Reeves