CNT5106C Computer Networks, Fall 2014
Homework #4: On the Network Layer and IP Multicast

Q1. (2 points) Is it necessary that every autonomous system use the same intra-AS routing algorithm? Why or why not?

A1. No. Each AS has administrative autonomy for routing within an AS.

Q2. (6 points) Compare and contrast the advertisements used by RIP and OSPF.

A2. With OSPF, a router periodically broadcasts routing information to all other routers in the AS, not just to its neighboring routers. This routing information sent by a router has one entry for each of the router's neighbors; the entry gives the distance from the router to the neighbor. A RIP advertisement sent by a router contains information about all the networks in the AS, although this information is only sent to its neighboring routers.

Q3. What is the 'rendezvous problem' in multicast? How can it be solved? (mention three main approaches/algorithms to the solution along with the protocols that use them)

A3. senders do not know about receivers and receivers do not know about senders (mainly for scalability purposes).
The main approaches to solve the rendezvous problem include:

1. broadcast and prune of multicast packets (truncated reverse path broacast, DVMRP, PIM-DM)
2. broadcast of membership information (MOSPF=OSPF + membership DB, and the use of Dijsktra's algorithm for routing)
3. use of a core or rendezvous point that the senders and receivers' first-hop-routers know about (CBT and PIM-SM)

Q4. (5 points) What is the difference between a group-shared tree and a source-based tree in the context of multicast routing?

A4. In a group-shared tree, all senders send their multicast traffic using the same routing tree. With source-based tree, the multicast datagrams from a given source are routed over s specific routing tree constructed for that source; thus each source may

have a different source-based tree and a router may have to keep track of several source-based trees for a given multicast group.

Q5. (10 points) What are the differences between the targeted environments (potential number of group members etc.) for PIM-DM and PIM-SM? How does this lead to different protocol design?

A5. In PIM-DM it is assumed that most parts of the network want to receive the multicast traffic. Therefore it starts with a flooding to build a complete multicast tree and later removes (or prunes) unwanted branches. Since most parts of the network want to receive the multicast traffic, it makes sense to have a routing state on all the routers for each group, as it would be useful with high probability.
In PIM-SM, on the other hand, it is assumed that most parts of the network do not want the multicast traffic. In stead of initial flooding, specific join mechanism is used in PIM-SM, and states are only created on routers that must know the state to forward the multicast traffic.

Q6. (10 points) In several multicast routing protocols we use RPF check (reversed-path forwarding check). What is the purpose of such check? How does it work? What are the underlying assumptions this check relies on?

A6. The purpose of RPF check is to avoid loops in multicast routing. We want to build a tree, which is loop-free, with the sender serving as the root. Hence a router only accepts incoming multicast traffic when it comes from the interface that is used to send packets toward the sender's IP address using the unicast routing table. By doing so a router only accepts incoming multicast traffic from each sender on one interface, and hence avoids the possibility of forming permanent routing loops.
The underlying assumptions of RPF check are:

(1) It depends on unicast routing table, so unicast routing table must be correct (and converged) for RPF checks to work properly.
(2) It assumes that the path used from a sender to a router and the reversed path from the router back to the sender are symmetric. If they are not, RPF check would reject multicast traffic on the shortest path from the sender to the router. It leads to non-optimal multicast tree.
    [Note: in cases where the links are uni-directional, then the reverse path approach can fail altogether.]

Q7. (11 points) IGMP provides membership information to the first hop router regarding the existence of receivers on a directly connected LAN.
(a) Why are group-specific query messages introduced in IGMPv2? Argue showing what a router does when it receives a 'leave' message from a host.
(b) The multicast host model does not define any interaction between the sources and IGMP. Do you see any problems with that? Explain. [Hint: Think of a case where there are no members for a group.]
(c) Suggest a simple modification to IGMP to solve the problem in (b).

A7. (a) (4 points) The group specific query is needed to query the LAN for membership in a certain group in case of a leave (IGMPv2 attempts to reduce leave latency by allowing explicit leave messages). A router receiving a leave message would trigger/send a query message that is group specific to the LAN. If the router does not receive any membership reports in response to this query it assumes there are no longer any members on that LAN and removes the LAN from its outgoing interface list.
(b) (4 points) The problem is that of network overhead. If there are no members in the group, then the source will keep on sending packets, and the leaf router (that has created a prune state) will keep dropping the packets on the floor. So the leaf network resources will be consumed unnecessarily (in terms of bandwidth and processing overhead in the leaf router).
(c) (3 points) One suggestion is to have IGMP send a 'no-member' report back to the source, if there are no members in the group (the leaf router for the source would know that from the prunes it gets in DVMRP or PIM register-stop messages in PIM-SM) [this approach is called reverse IGMP]

Q8. (12 points) Soft state vs. hard state

PIM-SM uses a concept called 'soft-state' in its messaging protocol. This concept simply indicates that a join message (for example) is sent periodically by the downstream routers to the upstream router to refresh the join state. An alternative would be to use 'hard-state' messaging, in which an ack is sent for each message, such that a join and a join-ack (2 messages) only need to be sent between an upstream and a downstream router on a link.

(a) Which protocol incurs less overhead on the network?

(b) Why are soft-state mechanisms sometimes preferred over hard-state mechanisms?

(c) *Extra:* Soft-state protocols incur more overhead on the network, especially when the number of states in the router (source-group pair state, for example)

increases, as a state refresh needs to be sent upstream for every state at fixed periods. Obviously, this approach does not scale. Suggest an approach to alleviate this problem and discuss its advantages and disadvantages. [Hint: You may use variable timers].

A8.

(a) (4 points) Soft state protocols incur periodic overhead to refresh the live states, while hard state only establishes the state using an 'acked' mechanism and it remains in place until/unless an explicity message removes it.

(b) (4 points) Soft-state protocols are more robust to network failures, in specific, router crashes. Since the soft state protocol uses periodic timers, the state can be re-created in a crashed router, by this periodic refresh. On the other hand, hard-state protocols do not recover gracefully from crashes, since they do not send periodic refreshes.

(c) (4 points) We can use the concept of 'scalable timers'. This concept states to keep the percentage of bandwidth allocated for control traffic fixed (e.g., keep control traffic to not more than 5% of the link bandwidth). As the number of states (that need to be refreshed) increases, the 'frequency' of refresh is decreased, and the refresh timers are 'scaled' (i.e., increased in value).
The advantage is to achieve more scalability by reducing control overhead. The disadvantage is that the refresh period will be increased, and so recovery time (after failure or crash) is increased, and join latency (incurred if the join message is lost for example) will be increased.

Q9. What is the timer-suppression mechanism, and why is it used? Mention at least two mechanisms for multicast routing (either in IGMP or multicast routing protocols) that use such a scheme.

A9. The timer suppression mechanism is used to counter the 'implosion' problem that may occur when multiple recipients of a multicast message attempt to respond almost simultaneously. Each node receiving the message sets a randomized timer, while the timer is running it listens for multicast messages. If the information that it wants to send has already been multicast then it suppresses its own transmission. Otherwise, it transmits the message after the expiration of the timer (more details in the lecture). IGMP uses this mechanism to suppress excess membership reports, and PIM-SM uses it to suppress multiple joins (from multiple downstream routers) on a LAN. Similarly

PIM-DM uses it to suppress multiple Join override messages on a LAN. (2 examples are sufficient).