

Internet Protocols Homework 4 Solutions

April 22, 2002

1 Question (a)

PIM is independent of the underlying unicast protocols unlike DVMRP and MOSPF. Advantages over DVMRP:

- PIM does not assume membership of routers by default, instead it requires interested routers to send explicit *join* messages. This is unlike DVMRP.
- PIM introduces a *rendezvous point* where receivers can learn about senders and senders can announce their existence. DVMRP causes a network-wide broadcast when a sender is ready.

Advantages over MOSPF:

- PIM allows both Shortest-path trees and shared-trees (those with a central point). In MOSPF the routing state requirement when there are large number of sources, can become prohibitively high.
- Broadcasting of membership information also impedes scalability of MOSPF.

2 Question(b)

The key deployment issues with IP multicast are handled by “EXPRESS” in the following manner.

- **Access Control:** Express requires the network layer of each receiver to present a *key* in order to join the channel. Thus unauthorised reception of data is avoided. The scheme allows only the source to transmit on to the channel, thus malicious users cannot stage flooding attacks.

- **Group Management:** A new mechanism called *CountQuery* is introduced which allows counting the number of subscribers among other quantities to handle billing. Also group creation is totally under the control of the source, using the authentication mechanism unwanted subscribers can be blocked.
- **Address Allocation:** Since each channel is addressed by a pair (S,E) where S is the sender's address and E is the channel destination address, each source on the Internet can maintain 2^{24} channels. So address duplication is an issue that is local to the source and easily avoided by maintaining a database of channels owned.

Deployment of ECMP is shown to be simple owing to a lot of the forwarding capabilities already implemented in multicast-aware routers.

3 Question(c)

- **TCP reliability and Digital Fountain:** TCP employs a reliability model based on retransmission of lost data as indicated by acknowledgements. Digital Fountain proposes a model where packets use special encoding schemes which help receivers recover the data without retransmissions. Digital Fountain is suitable when relying on ACKs becomes expensive (e.g., multicast, satellite links etc).
- **Efficiencies in video and data multicast:** A serious problem preventing the use of reliability in multicast is that of ACK implosion. By eliminating the need for ACKs and building alternate error recovery mechanisms, Digital Fountain immediately eases the problem of reliable multicast. Using what are known as Tornado codes, the scheme promises recovery of the entire original transmission if a particular number of packets are received. Specifically, if the information being multicast was composed of k packets and n packets were actually transmitted, Digital Fountain promises that the receiver can reconstruct the data by receiving any k packets.
- **Applications:** In general Digital Fountain can be used wherever the reverse channel bandwidth is very low or costly or non-existent. Examples include reliable multicast, dispersity routing, content mirroring etc.

4 Question(d)

- **Problems with transition to IPv6:** Due to the size of the installed base of IPv4 a simultaneous and controlled upgrade is not possible. So while some sites might upgrade to IPv6, there will be a lot of sites still running IPv4. In such a situation an isolated IPv6 site should be able to contact any other IPv4 or IPv6 site. Thus a transition mechanism must take care that an IPv6 site might have to pass through several IPv4 networks and vice-versa.
- **Solution proposed in RFC3056:** The 6to4 mechanism proposed in RFC3056 involves allocating an IPv6 prefix using the TLA reserved by IANA for the purpose of compatibility. Thus an IPv6 site can have a unique globally allocated IPv4 address and an IPv6 address generated using the IANA directives. So hosts within the IPv6 site see an IPv6 gateway. The global IPv4 address is used to encapsulate IPv6 packets when they have to traverse the IPv4 provider. The solution proposed is superior to the previous solutions since it does not need explicit tunneling or IPv4-compatible-IPv6 addresses.

5 Question II(a)

- **Differences between IPv4, IPv6, IPX, Decnet, Appletalk, CLNP:**
 1. Address format and length: **IPv4** - 4 bytes total, variable network ID, global registry; **IPv6** - 16 bytes total, global registry; **IPX** - 10 bytes total, 4 bytes network ID, 6 bytes host ID, no global registry; **Decnet** - 2byte address, 6 bit area ID and 10 bit host ID; **Appletalk** - 3 bytes total, 2 byte network ID, 1 byte host ID; **CLNP** - 20 bytes maximum, variable network ID of 1-12 bytes, 6 bytes host ID.
 2. Address resolution and configuration: **IPv4/IPv6** - Auto-configuration using DHCP servers and L2 address resolution using ARP; **IPX** - network ID obtained by listening to broadcasts from router, host ID obtained from IEEE address; **Decnet** - End nodes manually configured with network ID, host ID obtained by using HIORD method; **Appletalk** - Listen for broadcast messages from router for network ID, choose a random number in a particular range as

host ID; **CLNP** - Obtain network ID by listening to IS/ES-hello messages and use IEEE address to form host ID.

- **Advantages with IP over other network layer protocols:**

1. Address space: Unlike Decnet and Appletalk, the number of addressable hosts with IP compares with the scale of the Internet.
2. Address Hierarchy: Unlike CLNP where there is no topological significance to the Area-ID IP chose a hierarchical address which helped efficient routing across networks.
3. Global Registry: Unlike IPX, the network IDs in IP were chosen to be globally unique and a registry was entrusted with the job of allocating IP addresses.
4. Minimal L2 assumptions: Unlike Decnet where HIRDP method was used to resolve L2 addresses, or IPX and CLNP where IEEE address was part of the node ID, IP chose to remain independent of the nature of L2 by adapting ARP, thus allowing connectivity between heterogeneous networks.
5. Configuration: Although some protocols like IPX allowed for simpler end-host configuration, IP made up by using DHCP.

6 Question II(b)

- **Role of CIDR, NAT and DHCP:** The shortage of IP addresses can be remedied by reducing wastage of address space and by multiplexing addresses among multiple users.
 1. CIDR promotes efficient use of address space by allowing compaction of address ranges and flexible placement of class boundaries.
 2. NAT allows a network to use its own private IP addressing and employs address translation to map these private address to a few globally unique addresses when communicating with external networks.
 3. DHCP allows a site to multiplex a fixed number of IP addresses among multiple users by making address allocation dynamic. Given that the DHCP lease of an IP address expires after a fixed time, that address becomes available if the host is not using the address anymore.

- **IPv6 and DHCP:** Even though IPv6 has a big address space it needs DHCP as a stateful auto-configuration tool. With stateless configuration any host can connect to the network, while with DHCP the server can decide whether it allocates an address to the host. Also management of addresses for mobile devices is clean and easy with DHCP.
- **IPv6 and auto-configuration:** IPv6 endhosts use link-local addresses to multicast request for prefix information. If the network is managed by DHCP (*stateful autoconfiguration*) the router gives the prefix information and redirects the host to the DHCP server which allocates the address. Alternately, the host might generate a link-local address and connect to the network (*stateless autoconfiguration*). Address resolution is achieved by a generalization of ARP, by maintaining four caches. CLNP also uses Router, destination and neighbor caches. IPX and CLNP use the link-layer address and combine it with the advertised network prefix to obtain a node ID (similar to IPv6 stateless auto-configuration). Appletalk also has the idea of finding the best exit router.