Chapter 5

Anycasting

Anycast is defined as a standard service in IPv6 by Deering, S. and Hinden, R. (1998), although Partridge, C. and Milliken, W. (1993) had introduced it before for IPv4. However, anycasting is not originally proposed in the IPv4 protocol and its implementations are limited. A packet addressed to a group's anycast address is delivered to only one of the nodes in the group, typically the node with the "nearest" interface in the group, according to the routing protocol's measure of distances. Nodes in anycast groups are specially configured to recognize anycast addresses, which are drawn from the unicast address space (Hinden, R. and Deering, S., 1998).

5.1 Benefits of Anycasting

Jun-ichiro itojun Hagino and Ettikan, K. (2001) discuss about the benefits of anycast in their IETF Internet-Draft. Anycast service simplifies service location and configuration of nodes over IP network. With anycast, service location at the IP layer is simplified, without any special service protocols or implementation overheads. The selection of the nearest server using the protocols' measure of distance allows the nearest server to be discovered without user intervention for service provision. Selecting the nearest server can save bandwidth.

Assignment of single IP or service name addresses to similar services such as DNS, Network Time Protocol (NTP) and etc. can provide the generalization of services. The reliability of the service can be improved regardless of the failure of a single server and it is transparent to the user, as the user only has to remember the service name and not the IP addresses of all the servers.

Policy based routing is possible using anycast addressing architecture. An Internet Service Provider (ISP) can have his group of routers to be assigned an anycast to the interfaces. By using the Hop-by-hop routing option to specify the anycast address that a packet must traverse, the ISP can force the anycast packets to travel along his routers.

Using anycast can also be used in mobile networks to improve the mobile network architectures (Park, Vincent D. and Macker, Joseph P. 1999; Wei Jia et al., 1999).

5.2 Issues of Anycasting

Jun-ichiro itojun Hagino and Ettikan, K. (2001) discussed several issues regarding anycasting, they are as follows:

5.2.1 Limitations / Properties in the current Protocols

Identifying anycast destination

As the anycast address is allocated from unicast address space, so an anycast address is not distinguishable from a unicast address. Therefore a sender usually cannot identify if the node is sending a packet to anycast destination or unicast destination.

Nondeterministic packet delivery

If multiple packets carry an anycast address in IPv6 destination address header, these packets may not reach the same destination node, depending on the stability of the routing table. For example, in the case of fragmented IPv6 packets where each fragments may reach multiple different destinations and reassembly cannot be done.

Anycast address assignment to hosts

Hinden, R. and Deering, S. (1998) suggest assigning anycast address only to routers as there was no standard way for hosts to announce their intention to accept packets for anycast addresses. Besides, injecting host-routes may increase the size of the routing table entries considerably.

Anycast address in source address

As mention by Hinden, R. and Deering, S. (1998), IPv6 anycast address cannot be put into IPv6 source address typically because an IPv6 anycast address does not identify a single source node.

IPSec

IPSec and Internet Key Exchange (IKE) identify nodes by using source/destination address pairs. It is very hard to use IPSec on packets with an anycast address in the source address, destination address, or both. For manual keying, IPSec trust model with anycast address is confusing, as the same IPSec key has to be used for all anycast destinations that share an anycast address. Dynamic IPSec key exchange is complicated by the nondeterministic packet delivery of anycast. The security requirements to implement anycast are discussed in (Dondeti, L. et al., 2001).

5.2.2 Upper Layer Protocol Issues

UDP with anycast

Many of the UDP-based protocols use source and destination address pair to identify the traffic and it is not viable in the case of anycast, as it does not meet the requirement stated in IPv6 Addressing Scheme (Hinden, R. and Deering, S., 1998). (anycast address cannot be used as the source address of packets).

The suggestions given by Jun-ichiro itojun Hagino and Ettikan, K. (2001) to solve this issue are:

- The client should not check the source address of the incoming packet if using anycast address on the UDP protocol exchange. Packet pairs must be identified by using UDP port numbers or upper-layer protocol mechanisms.
- Verify the authenticity of the reply for secure UDP protocol exchange, by using upper-layer security mechanisms like DNS Security (DNSSEC).

TCP with anycast

TCP exchanges cannot simply be used with anycast addresses as a TCP connection is identified using unicast address/port pair for the source/destination node. To enable the use of IPv6 anycast in TCP, it is desirable to implement some of the following:

- Define a TCP option, which allows switching of peer's address from IPv6 anycast address to IPv6 unicast address.
- Define an additional connection setup protocol that resolves IPv6 unicast address from IPv6 anycast address. The IPv6 unicast address is resolved using the new protocol and then a TCP connection is made using the IPv6 unicast address.

5.3 Works on Anycasting

Although there are several recent studies on anycasting, many of them are not meant to improve the performance of the anycast routing protocols itself. Debates on the building of the anycast routing protocol are still ongoing.

A typical anycast routing protocol must be a loop-free routing protocol that can selects the "nearest" interface having the anycast group members, according to the protocol's measurement of distances. Basically there are two approaches in the building an anycast routing protocol: single-path routing and multi-path routing.

Park, Vicent D. and Macker, Joseph P. (1999b) proposed several extensions to the existing unicast routing protocols to provide anycast services. Extensions to link-state, distance-vector and link-reversal unicast routing protocols are all conceptually realized through the representation of an anycast service as a "virtual node" in a graph based on the network topology. This terminology is adopted in this thesis to provide an extension to the Routing Information Protocol next generation (RIPng) for IPv6 (Malkin, G. and Minnear R., 1997).

Global IP-Anycast (GIA) introduced by Katabi, D. and Wroclawski, J. (2000) dividing the inter-domain anycast routing into two components. The first component builds some default anycast routes (popular) and the second component controlled by the edge domains generates anycast routes (unpopular) according to the domain's interests. Searching of popular anycast route will be able to be performed directly, but scoping searches will have to perform for the unpopular anycast routes. GIA tries to cater for the issues of host-anycasting in global IP environments by reducing the number of routes in the Internet backbone routers. The drawback of the GIA is the single-path routing approach might lead to congestion happening at certain nodes (especially the nodes providing the services) in the Internet although there are some other available nodes.

Several anycast routing protocol reviewed by Dong Xuan et al. (2000) are Shortest-Shortest Path Method, Minimum Distance Method, Source-Based Tree Method and Core-Based Tree Method. Single-path routing and multi-path routing issues are discussed in the paper. According to Dong Xuan et al. (2000), the problem associated with single-path routing is that it may overload the selected path and hence cause traffic congestion and the multi-path routing is proposed to address this problem. However the problems faced by the Core-Based Tree Method such as poor core placement and traffic concentration around the core router, pointed by Katabi, D. (1999) are not discussed.

An integrated routing algorithm for anycast messages introduced by Wei Jia et al. (2000a) is attempting to use both single-path and multi-path routing algorithm in anycast routing. A number of routers, which are heavily loaded, will be using multi-path routing and the rest of the routers will be using single-path routing. This algorithm tries to solve a potential problem of a multi-path routing, which is the increase of packet delay at router due to the time taken to swap-in/out the entries in routing table in the process of re-establishing routing entries, when the memory size of a router is limited. However, this algorithm has its drawback. The use of source-based tree method in this algorithm, rather than the preferred core-based tree method may introduce more overheads to the traffic.

Besides these works discussed before, there are several works done by Katabi, D. (1999) and Wei Jia et al. (2000b). However, they are intended to use anycast routing to improve the efficiency of the multicast routing rather than improving the anycast routing protocol itself.