Neighbour Discovery in IPv6

Andrew Hines

Topic No: 17

Email: hines@zitmail.uni-paderborn.de

Organiser: Christian Schindelhauer

University of Paderborn

Immatriculation No: 6225220

August 4, 2004

Abstract

IPv6 is the new network layer protocol, which is sought to eventually replace the existing IPv4 protocol as the standard of choice used throughout the global internet. Brought about initially due to urgent requirement for more available IP addresses, IPv6 also aims to provide substantial improvements on the old protocol and introduce entirely new innovations. One such improvement which includes innovative new solutions is the Neighbour Discovery protocol of IPv6. It is the implementation of this protocol and the services it provides which are the primary focus of the following report, and also how it improves on the current level of service that equivalent IPv4 protocols provide.

1 Introduction

IPv6, or IPng (new generation), is the new protocol designed to take over from IPv4, as the Network Layer utilised throughout the global internet. Although IPv4 has served well in its time, and continues to do so, its design did not foresee how immensely large the internet would become and all of the many various applications which would eventually depend upon it. Because of the massive growth of the internet and the proliferation of internet-connected devices other than typical computers (e.g. mobile phones, PDAs), the number of available IPv4 addresses (over 4 billion in total from an IP address length of 32 bits) is dwindling. This is also not helped by the method in which IPv4 addresses are structured into network and host components, leading to potential addresses being wasted.

IPv6 addresses are 128 bits in length (allowing for more than 3×10^{38} addresses), which more than compensates for the limited availability of IP addresses available in IPv4. The large address size also means that addresses can have a much more structured hierarchy than what IPv4 addresses are able to provide. The new improved IP standard also sets out to improve other aspects of the IPv4 specification and implement new services. One such improvement which also implements some new services, involves the implementation of the Neighbour Discovery protocol[7] in IPv6.

The protocol provides the following services in IPv6[7]:

- Allows nodes (hosts and routers) to determine the link layer addresses of nodes residing on the same network link to facilitate next-hop delivery of packets
- Allows hosts to locate neighbour routers, and be redirected to a better choice of router for a given IPv6 destination address
- Provides mechanisms to assist in the autoconfiguration of IPv6 nodes
- Enables nodes to track the reachability state of its neighbours

It is the Neighbour Discovery protocol which remains the focus of this report. The report is structured as follows. It begins with an overview of IPv6 addresses and their format and structure. It then looks at the data structures and message types used within Neighbour Discovery. The services of Neighbour Discovery are then investigated in detail, and in particular, how they are utilised within the host autoconfiguration procedure for a node's interface and the packet transmission algorithm. The report concludes with a high level comparison with current IPv4 implementations.

2 IPv6 Addresses

It is important to consider the structure and representation of IPv6 addresses[5] in order to understand their implementation within the Neighbour Discovery Protocol. The following section discusses these attributes, and also gives examples of IPv6 addresses that are used within the Neighbour Discovery Protocol.

As mentioned before, one of the main reasons for the IPv6 address representation in 128 bits was to massively expand the number of available addresses. In doing so, this allowed IPv6 addresses to have a much more flexible hierarchical structure, leaving enough address space to enable the use of global addresses for the internet and local addresses for intranets[3].

IPv4 addresses are structured to identify a separate network and host address. It is the network address that allows hosts belonging to that network to be reachable over the internet. The network address component can be then further subdivided into subnetworks, using a netmask parameter to differentiate between them. Nodes on the same subnetwork are considered to be neighbours, i.e. nodes attatched to the same link, and are able to communicate directly.

In IPv6, the netmask is replaced by a prefix which indicates how many bits of the address are assigned to a subnetwork. The remaining bits may be then assigned to nodes within the subnetwork. It should be mentioned here that IP addresses are assigned to network interfaces of nodes and not the node itself[3].

2.1 Address Format

The 32 bits of IPv4 addresses are represented via unsigned integers split into 4 octets, and separated by dots. Each octet can therefore represent a possible 256 values.
Here is an example: 212.190.45.3

IPv6 addresses on the other hand, are 128 bits in length, and therefore using the same representation model as IPv4 would result in a horrendously long address (visually). Thus, the decision was made to consider the 16 octets of an IPv6 address as 8 unsigned integers and writing each number with 4 hexidecimal digits separated with colons[5].
For example: 1080:0000:0000:0000:0008:0800:200C:417A

In the given example above, the address representation may be compressed by eliminating leading zeros within each octet and eliminating series of octets containing zeros (although this can only be applied once to an address[5]).
So our previous IPv6 address now becomes: 1080::8:800:200C:417A
Note that where a series of zeroed octets was previously, we now use two adjacent semicolons.

As mentioned before, an IPv6 prefix identifies how many bits of the address are assigned to the subnetwork. It is represented by the notation: IPv6 address/prefix length.
For example: 1080:0:0:0:8::/80 displays a subnet with an 80-bit prefix.
As another example, a node address of 12AB:0:0:CD30:123:4567:89AB:CDEF
with a prefix of 12AB:0:0:CD30::/60
can be abbreviated as 12AB:0:0:CD30:123:4567:89AB:CDEF/60

2.2 Addressing Model

In the Neighbour Discovery protocol, 2 main address types are used[7], as discussed below. The unicast address belongs to a single interface of a node. Packets forwarded to this address are delivered only to the interface identified by that address.

The multicast address belongs to a set of interfaces, usually belonging to different nodes. Packets forwarded to this address are delivered to all interfaces belonging to the set[2].Multicast addresses replace broadcast addresses utilised in IPv4, and their use may facilitate a reduction in network traffic in comparison to the use of broadcasting in IPv4[3].

Many kinds of unicast and multicast addresses exist[5]. To identify which class a particular address belongs to, a variable length format prefix is present in the beginning bits of the address[5]. We now look at specific examples of unicast and multicast addresses that are important with regard to the Neighbour Discovery Protocol.

2.3 Unicast Addresses

Aggregatable Global Unicast address

This address is the address of a node's interface that is presented to the global internet and thus identifies a unique node on the internet. Its format prefix value is 001. The entire address is split into three main ID components. The first is the subscriber ID which identifies a set of addresses an organization has been allocated. The subnet ID splits this set into many subnets. Finally, the Interface ID is the link layer address of the interface (e.g. its MAC address).

Link Local Address

This address is known only to other nodes which exist on the same link. Its format prefix value is 1111 1110 10. The local link address is very important for use in the Neighbour Discovery protocol. It is constructed simply by concatenating the prefix FE80:: with the node's link layer (interface) address.

The Unspecified Address

This address consists completely of zeroes and therefore requires no prefix. It can be written in compressed form as "::". It is not assigned to interfaces, but rather used as a source address in packets sent when a node is attempting to obtain an IPv6 address.

2.4 Multicast Addresses

All variations of multicast addresses begin with the format prefix of 1111 1111. The multicast address structure is as follows. The first 8 bits contain the format prefix. A following flags field can indicate whether this multicast address has been permanently assigned.

The following scope field limits the scope of the multicast group. This scope may be restricted, for example, to interfaces on the same node, the same link, the same organisation, or the global internet. The examples of multicast addresses we will examine all have a scope limited to the same link, as this is the domain in which the Neighbour Discovery protocol operates. The remaining 112 bits represent the group ID, identifying the multicast group.

All Nodes Multicast Address

This address identifies all nodes within the link local scope, and is expressed as FF02::1.

All Routers Multicast Address

This address identifies all routers within the link local scope, and is expressed as FF02::2.

Solicited Node Multicast Address

This address is reserved specifically for the Neighbour Discovery Protocol within a link[7]. This type of multicast address can occur in the range from FF02::1:FF00:0000 to FF02::1:FFFF:FFFF. The address is formed by appending the lower 24 bits of the unicast address to the prefix FF02::1[5]. A node must compute and join the associated Solicited Node multicast addresses for every unicast address that is assigned to it.

3 Neighbour Discovery Protocol

The Neighbour Discovery protocol is detailed in a document put forward by the Internet Society, an organisation responsible for developing standards to be used in the global internet. This document is called "RFC2461" and is currently in its draft standard[8], as is RFC2460[8] which specifies the IPv6 protocol. Draft standard implies that working implementations are available and that they have been thoroughly tested[4].

The Neighbour Discovery protocol manages interactions between nodes via message exchanges[6]. These messages provide the data necessary for the processes of host autoconfiguration and packet transmission on a local link[6].

Host autoconfiguration[6] involves the separate tasks of:

- Parameter Discovery, which is facilitated through the Router Discovery process. Here, the necessary parameters required for host autoconfiguration are obtained.
- Address Autoconfiguration
- Duplicate Address Detection, which detects the presence of duplicate addresses on the same link.

The packet transmission process[6] requires data which can be obtained via the following processes:

- Router Discovery, whereby a host locates routers which reside on the same local link
- Prefix Discovery, which is implemented through Router Discovery and provides the set of on-link prefixes
- Address Resolution, the process of resolving a neighbour's destination address to its link layer address and thereby enable the local delivery of packets
- Neighbour Unreachability Detection, responsible for determining if a neighbour can be reached
- Redirect, whereby a router informs the host of a better router on the local link to be used to forward packets to a given destination

Another protocol, ICMPv6[1] (also in draft standard[8]), defines messages which among other things, are used to aid in facilitating the services that Neighbour Discovery provides[7]. These messages are further discussed in the following paragraphs.

3.1 ICMPv6 Messages

Router Advertisement

Routers use these messages to inform other nodes existing on all links to which they are connected, of their presence. The process occurs periodically or in response to a Router Solicitation message. These messages also provide other link related information. Through Router Advertisements, a host can build its default router list automatically, and thus overcome the limitation of the manual configuration of the default router in IPv4.

Router Solicitation

Upon the enabling of an interface of a node, these messages can be used to request all routers on the same local link to send Router Advertisements immediately, rather than waiting until the next periodically scheduled advertisement.

Redirect

These messages are used by routers to tell hosts that a better on-link router exists for a given destination address.

Neighbour Solicitation

These messages have 3 main purposes. The first is to discover the link layer address of a neighbour as part of the address resolution process. This process replaces the use of ARP requests and replies in IPv4. The second purpose is to determine the reachability of a neighbour. The last is to detect the presence of duplicate IPv6 addresses during the address autoconfiguration process which is detailed later in this report.

Neighbour Advertisement

These messages are either in response to Neighbour Solicitations, or sent by a neighbour to announce a change in its link layer address. Upon receipt of a Neighbour Advertisement, a node will update its neighbour cache which contains mappings between IPv6 and link layer addresses of neighbours.

3.2 Caches used in Neighbour Discovery

There are four main data structures a node must have and maintain to assist in Neighbour Discovery protocol services[7]. These caches are illustrated in Figure 1. It should be noted that these

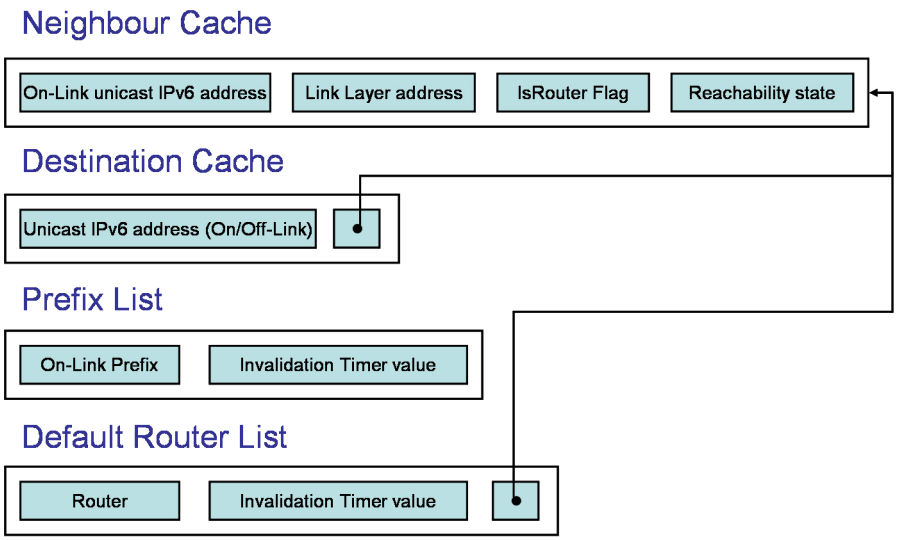

Figure 1: Caches used in neighbour discovery.

data structures are conceptual, and could be implemented within nodes in a variety of ways[7]. We now look at each of them in turn.

Neighbour Cache

This contains a set of entries regarding neighbours to which packets have been recently sent. The data fields contained within it are the neighbour's on-link unicast IP address, its link layer address, a flag to indicate if the neighbour is a router, and data pertinent in determining its reachability. The cache also contains a pointer to queued packets which are waiting to be sent to the neighbour.

Destination Cache

This cache contains a set of entries regarding destination addresses to which packets have been recently sent. An entry contains the destination address (on- or off-link) and a pointer to the relevant entry in the neighbour cache, which contains details regarding the next-hop on route to the given destination. The destination cache is updated upon receipt of ICMPv6 Redirect messages.

Prefix List

This is a list of prefixes that define a set of on-link IPv6 unicast addresses. Entries are initiated upon receipt of data contained in Router Advertisements. Each entry has an invalidation timer value, which cause the expiration of invalid prefixes. Link local prefixes have an infinite value in this field, and thus never expire.

Default Router List

This is a list of the routers to which packets may be sent. Each entry contains an identifier for the router, its invalidation timer value which is obtained from Router Advertisements, and a pointer to the relevant entry in the neighbour cache. The algorithmic choice of a default router is known to favour those which are determined as reachable. Once a router entry becomes "invalid", it is deleted from this cache.

3.3 Host Autoconfiguration

When the link layer interface of a host is first connected to the network it must acquire information necessary for the host to communicate on the local link and the entire network. It must obtain Local Link and Aggregatable Global unicast IPv6 addresses, a list of on-link routers, a list of on-link prefixes, and other related information[7]. The entire process of Host Autoconfiguration[6] is depicted in Figure 2.

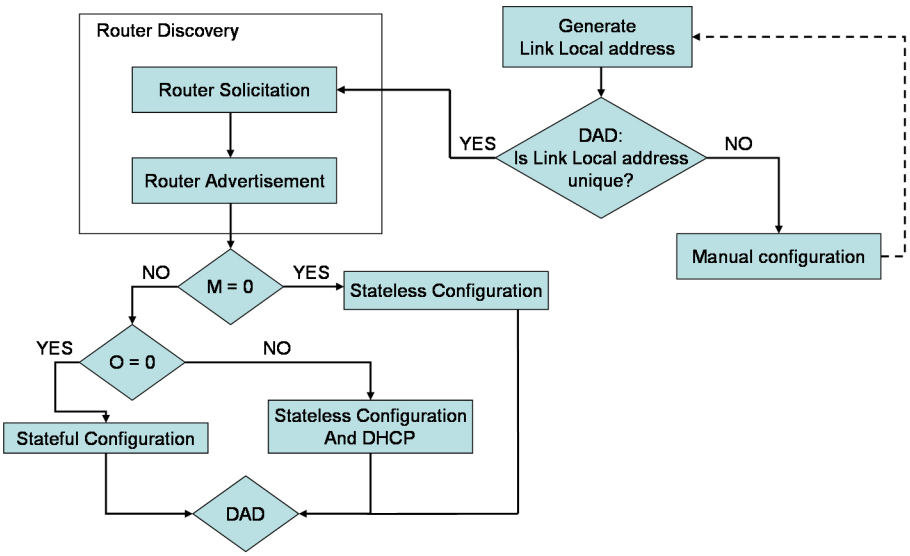

Figure 2: Host autoconfiguration[6].

The process begins with the automatic generation of a link local IPv6 address as described in Section. Since it is also possible to manually configure link layer addresses, there is a chance that a duplicate link local address exists on the same link of the network. To determine if this is the case, the Duplicate Address Detection procedure[7] is invoked.

Duplicate Address Detection

The host interface to be auto-configured sends a Neighbour Solicitation to all node interfaces on the same link belonging to the same solicited node multicast address. This type of multicast address ensures that the Neighbour Solicitation will only be received by member nodes of the same multicast group (i.e. those that match in the last 24 bits of their IPv6 address). The source address included in the IPv6 header is the unspecified address. The target address field of the Neighbour Solicitation contains the link local address which is to be checked for duplication.

If no host responds within a given time period, the host undergoing autoconfiguration may keep its link local address. Otherwise, the host containing the duplicate address responds with a Neighbour Advertisement. This advertisement is sent to all nodes on the same link by using the all nodes multicast address as its IPv6 destination address. The message contains its link layers address and a flag to indicate if the responding node is a router (hereon referred to as IsRouter flag).

All nodes on the same link will therefore be forced to update their neighbour caches if their entries are not up-to-date. Receipt of a Neighbour Advertisement also updates the reachability status entry in the neighbour cache. A duplicate address on the local link may require the manual configuration of the new host interface link local address[6].

Router Discovery

Once a unique link local address has been obtained, the newly connected host needs to discover routers on its local link and also prefix lists which are used on the local link. This is performed in the next stage of autoconfiguration: Router Discovery[7].

The newly connected host sends out a Router Solicitation to all routers on the local link using the all router multicast address as the destination address. In doing so, the host provides all such routers with its newly created local link address and its corresponding link layer address, so that all routers may update their records. All routers then respond in turn with a Router Advertisement. This message contains the following important data to be used by a host in the autoconfiguration process:

- A router's link layer address
- A router's lifetime (i.e. how long a host is able to keep using this router until subsequent advertisements update this value)
- Flags used to determine the process by which the host's aggregatable global unicast address is created
- Periodical timer values used in the Address Resolution and Neighbour Unreachability Detection procedures
- Prefixes which should be cached in the host's prefix list

Extra prefix related data may also be included in the advertisement message, including:

- L (On-link) flag: when set, this prefix can be used to determine if a node containing this prefix is on-link
- A (Autonomous Address Configuration flag): when set, the prefix may be used for stateless configuration of the host's aggregatable global unicast address
- The valid and preferred lifetimes of a prefix

Upon receipt of the Router Advertisements, a host updates the relevant fields of its default router list, neighbour cache and prefix list. Now the host has the link local IPv6 and link layer addresses of all on-link routers, a list of on-link prefixes, and other relevant data.

Autoconfiguration of aggregatable global unicast address

There are 2 flags which together determine how the host's aggregatable global unicast address is created[7]. These are:

- M (Managed Address Configuration) flag
- O (Other Stateful Configuration) flag

This process of determination can be seen in Figure 2. Stateless configuration of an address involves concatenating a valid prefix with the host's link layer address[3]. Full stateful configuration requires the use of the Dynamic Host Configuration Protocol (DHCPv6) to configure the host's aggregatable global unicast address on its behalf[6]. The final alternative is to configure the address using the stateless method, but using DHCPv6 for additional parameters[6].

3.4 Packet Transmission Algorithm

Now that a node has both a local link address and an aggregatable global address, a default router list and a list of on-link IPv6 address prefixes, it is able to effectively communicate with other nodes on the same link or across the global internet. The process of packet transmission[6] from such a host node is now depicted in Figure 3. and should be referred to repeatedly throughout the following discussion on the packet transmission process. The best-case situation for packet

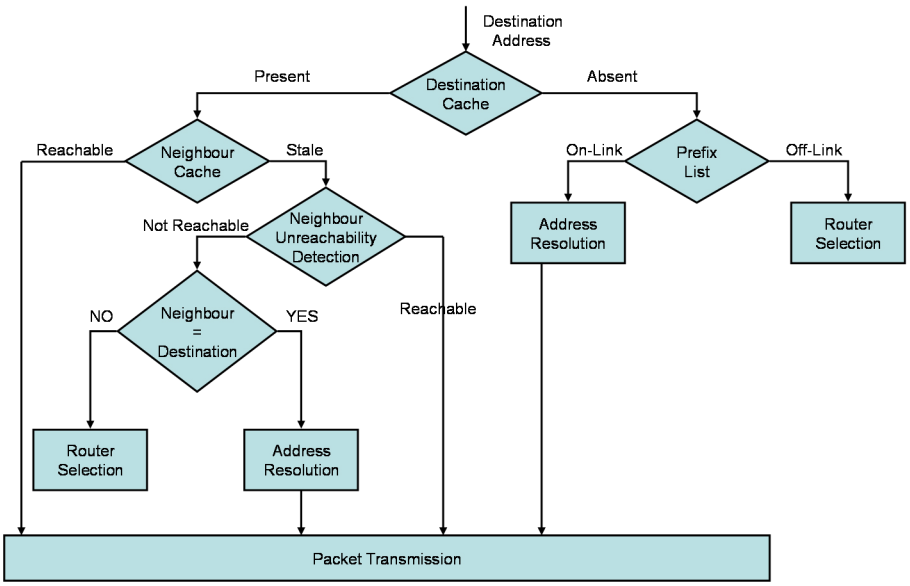

Figure 3: The packet transmission algorithm[6].

transmission is when both the destination address and the next-hop (neighbour) address for this destination are present in the host's destination and neighbour caches respectively. If the entry for the neighbour is also determined as reachable, the queued packet can be transmitted immediately. If the entry is marked as stale, it means that no Neighbour Advertisements or other acknowledgements from higher level protocols (such as TCP) have been received from the neighbour within a specified time period. At this point the host must determine the neighbour's reachability status via the Neighbour Unreachability Detection mechanism[7].

Neighbour Unreachability Detection

The node wishing to determine a neighbour's reachability sends a Neighbour Solicitation to the neighbour. The solicitation contains the link layer address of the source node, should the neighbour

be reached and need to update its neighbour cache entry for the source node. If the neighbour is reached, it replies with a Neighbour Advertisement, and the source node must then update the cached entry for this neighbour upon its receipt. The queued packet may now be sent to the neighbour.

If no advertisement is received within a given time period, the neighbour entry is deleted from the source node's neighbour cache. If the destination address was in fact a neighbour, the process of Address Resolution is required to rediscover its link layer address and then transmit the packet. If the destination is not a neighbour (i.e. it is off-link) then a router must be chosen randomly from its router list to attempt the packet delivery. The Router Redirect process is invoked at this stage if necessary. Both Address Resolution[7] and Router Redirect[7] are investigated further at this point.

Address Resolution

The node which wishes to discover the link layer address of a neighbour, sends a Neighbour Solicitation to all nodes which belong to the same solicited node multicast group. The message contains the link local address of the "target node", and the link layer address of the node sending the solicitation. When the neighbour is found, it responds to the sending node with its link local address contained within a Neighbour Advertisement. The sending node then updates the link layer address and reachability status of the responding neighbour in its neighbour cache.

Router Redirect

When a node chooses an on-link router randomly from its default router list to forward a packet, there is a good chance that this choice of router is not the best with regard to the ultimate destination address. If this is the case, the router (say R1) receiving the packet to be forwarded will determine from its routing table that there exists a better on-link router for this destination. It will relay the packet to the "better choice" router (say R2) which will in turn forward the packet.

R2 then sends a Redirect message to the host from which the packet originated. This Redirect message informs the original host that R2 is the best choice router for this particular destination address, and the host updates the link local and link layer addresses in its neighbour cache that are pointed to by the destination cache entry.
Up until now, we have assumed that the destination address of the packet to be delivered was cached by the sending host. Thus far we have traversed the entire left hand side of Figure 3. We now make the assumption that the destination address is not cached by the sending host and begin our traversal of the right hand side of the packet transmission algorithm represented in Figure 3.

When such a situation exists, the prefix list of the sending node can be consulted to verify that the destination is on- or off-link. If it is on-link, then the destination is a neighbour and its link local address can be obtained via Address Resolution. The packet can then be delivered to its destination.

If however, the destination is off-link a router must be selected from the sending node's default router list to forward the packet onto the off-link destination. Since no entry exists in the destination cache for the destination, a router must be randomly chosen to forward this packet and the Redirect process may have to be initiated as before if the router chosen was not the best choice.

4 Comparison with IPv4 Implementation

The Neighbour Discovery protocol of IPv6 attempts to improve on the corresponding facilities that are currently provided in IPv4, as well as introduce completely new innovative services. In IPv4 the Address Resolution Protocol (ARP) performs the duties of Address Discovery, ICMP Router Discovery (RDISC) performs the duties of ICMPv6 Router Discovery, and ICMP Redirect (ICMPv4) substitutes for ICMPv6 Redirect[7]. The Neighbour Unreachability Detection as implemented in IPv6 Neighbour Discovery is, for the most part, a new innovative service[7]. Some of the improvements provided by Neighbour Discovery in IPv6[7] are summarised as follows.

4.1 Router Discovery

In Neighbour Discovery, this service is provided as a core element of the protocol, whereas in IPv4 routing protocols had to be monitored in a fashion which was not central to any specific protocol. ICMPv6 Redirect messages contain the link layer address of the better choice first-hop router, whereas in IPv4 a separate address resolution stage is required to obtain the link layer address of such a router.

4.2 Router Advertisements

The link layer address of a router is carried in the ICMPv6 Router Advertisement, therefore no subsequent exchange of packets is required for Address Resolution of the router. Router Advertisements carry on-link prefixes, whilst in IPv4 a separate procedure is required to configure netmasks (the IPv4 equivalent of prefixes). The concept of address autoconfiguration is completely new in IPv6, and facilitated through ICMPv6 Router Advertisements. In the event of site renumbering, where the organisational network is assigned new global prefixes, on-link router associations are maintained by using link local addresses to identify them.

4.3 Address Resolution

The use of multicasts in IPv6 Address Resolution instead of broadcasts in IPv4 ARP, reduces considerably the amount of traffic directed to nodes other than the target. Additionally, co-existing IPv4 nodes should not be interrupted at all by IPv6 multicasts.

5 Summary

The Neighbour Discovery protocol of IPv6 is a focussed attempt at combining a number of corresponding IPv4 protocols into one central protocol. It is utilised heavily to support host autoconfiguration and the packet transmission process within a local link. It seeks to solve problems related to these processes in a manner that is most efficient with regard to time and resources, and offer a substantial improvement over equivalent IPv4 solutions.

How successful the IPv6 protocol, and with it Neighbour Discovery, proves to be remains to be seen. It will be many years yet before the global internet rids itself of the old and makes way entirely for the new. In this time, co-existence and convergence of both protocols remain substantial challenges. Challenged that exist now and are likely to remain in the future.

References

[1] A. Conta and S. Deering. Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification. RFC 2463, The Internet Society, December 1998. http://www.faqs.org/rfcs/rfc2463.html.

[2] S. Deering and R. Hinden. Internet protocol, version 6 (ipv6) specification. RFC 2460, The Internet Society, December 1998. http://www.faqs.org/rfcs/rfc2460.html.

[3] S. Gai. *Internetworking IPv6 with Cisco Routers*. McGraw Hill, first edition, 1998.

[4] Cecil Goldstein. Internetworking (itb524) lecture notes. Queensland University of Technology lecture notes, July 2002.

[5] R. Hinden and S. Deering. Ip version 6 addressing architecture. RFC 2373, The Internet Society, July 1998. http://www.faqs.org/rfcs/rfc2373.html.

[6] Telecom Lab Italia. The neighbour discovery protocol. http://www.ngnet.it/e/ipv6proto/ipv6-proto-6.php.

[7] T. Narten, E. Nordmark, and W. Simpson. Neighbor discovery for ip version 6 (ipv6). RFC 2461, The Internet Society, December 1998. http://www.faqs.org/rfcs/rfc2461.html.

[8] rfc editor. The neighbour discovery protocol, August 2004. http://www.rfc-editor.org/rfcxx00.html.