specifies *P*'s Ethernet address as the hardware address. *R* will receive the reply, place it in the ARP cache, and send an IP packet to *P* (because *P* has impersonated H_4). When it receives an Internet packet, *P* examines the destination address in the packet, and forwards the packet to H_4.

Proxy ARP also handles impersonation and forwarding when a computer on network 2 sends to a computer on network 1. For example, when H_4 forms an Internet packet and needs to send the packet to router *R*, H_4 will broadcast an ARP request for *R*. *P* will receive a copy of the request, consult its database, and send an ARP reply that impersonates *R*.

How can proxy ARP be used for security? Proxy ARP can be used for a firewall or on a VPN connection. The idea is that because a proxy ARP machine impersonates machines on the second network, all packets must travel though the proxy ARP machine where they can be checked. In Figure 6.4, for example, a site could place all hosts on network 2 and put firewall software in machine *P*. Whenever a packet arrives from the Internet, the packet will go through *P* (where the packet can be examined and firewall can be rules applied) on its way to the destination host.

6.18 IPv6 Neighbor Discovery

IPv6 uses the term *neighbor* to describe another computer on the same network. IPv6's *Neighbor Discovery Protocol* (*NDP*) replaces ARP and allows a host to map between an IPv6 address and a hardware address†. However, NDP includes many other functions. It allows a host to find the set of routers on a network, determine whether a given neighbor is still reachable, learn the network prefix being used, determine characteristics of the network hardware (e.g., the maximum packet size), configure an address for each interface and verify that no other host on the network is using the address, and find the best router to use for a given destination.

Instead of creating a protocol analogous to ARP to handle neighbor discovery, the designers of IPv6 chose to use ICMPv6‡. Thus, ICMPv6 includes messages that a computer uses to find its neighbors at startup and to check the status of a neighbor periodically.

A key difference between ARP and NDP arises from the way each handles the status of neighbors. ARP uses a late-binding approach with soft state. That is, ARP waits until a datagram must be sent to a neighbor before taking any action. After it performs an exchange, ARP stores the binding in its cache, and then sends IP packets to the neighbor without checking the neighbor's status until the ARP cache timer expires. The delay can last many minutes. NDP uses early binding and takes a proactive approach to state maintenance. Instead of waiting until a datagram must be sent, an IPv6 node uses NDP to discover neighbors at startup. Furthermore, an IPv6 node continually checks the status of neighbors. Thus, transmission of an IPv6 datagram to a neighbor can proceed without delay and does not involve broadcast.

†See Chapter 22 for a discussion of NDP.
‡See Chapter 9 for a discussion of ICMPv6.